Avocent

SwitchView® IP 1020
Remote Access Device

Installer/User Guide

USA Notification

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Canadian Notification

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Japanese Notification

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Korean Notification

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.

Safety and EMC Approvals and Markings

UL, FCC, cUL, ICES-003, CE, VCCI, MIC, C-Tick

SwitchView® IP 1020 Remote Access Device

Installer/User Guide

Avocent, the Avocent logo, The Power of Being There, SwitchView, DSView, Dambrackas Video Compression and OSCAR are registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2008 Avocent Corporation. 590-538-616E

Instructions

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Power On

This symbol indicates the principal on/off switch is in the on position.

Power Off

This symbol indicates the principal on/off switch is in the off position.

Protective Grounding Terminal

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

List of Figures ..... **vii**

List of Tables ..... **ix**

Chapter 1: Product Overview **1**

Features and Benefits *1*

Accessing a remote access device via network connection *1*

Simple access to a target device *1*

Chapter 2: Installation **3**

SwitchView IP 1020 Remote Access Device Connectivity *3*

Installation Overview *3*

Getting started *5*

Setting up your network *5*

Connecting the Remote Access Device Hardware *5*

SwitchView IP 1020 remote access device LEDs *6*

Adjusting Mouse Settings on Target Devices *6*

Chapter 3: Web Interface Operations **9**

On-Board Web Interface *9*

Logging into the SwitchView IP 1020 remote access device *10*

The SwitchView IP 1020 Explorer Window *11*

Using the side navigation bar *12*

Using the top option bar *13*

Managing local accounts *14*

Managing device properties *14*

Configuring LDAP *15*

LDAP Overview parameters *16*

LDAP Search parameters *17*

LDAP Query parameters *19*

Appliance and Target Device Query Modes *21*

Setting up Active Directory for performing queries *23*

Rebooting the appliance *24*

Managing local accounts *24*

Access levels *24*
Preemption levels *25*

Chapter 4: The Video Viewer 27

The Video Viewer Window *27*
Launching a KVM Session *28*
Session time-out *28*
Video Viewer Window Features *28*
Changing the toolbar *30*
Setting the window size *30*
Adjusting the view *30*
Adjusting color depth *32*
Additional video adjustment *32*
Target video settings *33*
Contrast and brightness *34*
Detection thresholds *34*
Block Noise Threshold and Pixel Noise Threshold *34*
Automatic video adjustment *34*
Refresh Image *35*
Video Test Pattern *35*
Adjusting mouse options *35*
Cursor type *35*
Mouse scaling *37*
Vendor-specific video settings *37*
Mouse alignment and synchronization *37*
Using Keyboard Pass-through *38*
Using Macros *38*
Saving the View *39*
Closing a Video Viewer Window Session *39*

Appendices 41

Appendix A: Flash Upgrades *41*
Appendix B: Technical Specifications *43*
Appendix C: Sun Advanced Key Emulation *45*
Appendix D: Reset to Factory Defaults *47*

Appendix E: Technical Support *48*

LIST OF FIGURES

Figure 1.1: Example SwitchView IP 1020 Remote Access Device Configuration *2*
Figure 2.1: Basic SwitchView IP 1020 Remote Access Device Configuration *4*
Figure 3.1: SVIP 1020 Explorer (User Login) Screen *11*
Figure 3.2: Avocent SwitchView IP 1020 Explorer Window *12*
Figure 3.3: LDAP Overview Page in the OBWI *17*
Figure 3.4: LDAP Search Page in the OBWI *18*
Figure 3.5: LDAP Query Page in the OBWI *20*
Figure 3.6: Active Directory - KVM User *21*
Figure 3.7: Active Directory - KVM Appliance Admin *22*
Figure 3.8: Active Directory - Define Groups *23*
Figure 4.1: Video Viewer Window (Normal Window Mode) *29*
Figure 4.2: Manual Video Adjust Dialog Box *33*
Figure 4.3: Video Viewer Window with Local and Remote Cursors Displayed *35*

LIST OF TABLES

Table 1.1: Descriptions for Figure 1.1 ..... *2*
Table 2.1: Descriptions for Figure 2.1 ..... *5*
Table 3.1: On-Board Web Interface Supported Operating Systems and Browsers *9*
Table 3.2: Descriptions for Figure 3.2 ..... *12*
Table 3.3: Viewing Appliance Information *15*
Table 3.4: Allowed Operations by Access Level *25*
Table 4.1: Descriptions for Figure 5.1 ..... *29*
Table 4.2: Descriptions for Figure 5.2 ..... *33*
Table 4.3: Descriptions for Figure 5.3 ..... *36*
Table B.1: SwitchView IP 1020 Remote Access Device Product Specifications *43*
Table C.1: Sun Key Emulation *45*
Table C.2: PS/2-to-USB Keyboard Mappings *46*

CHAPTER 1

Product Overview

Features and Benefits

The Avocent SwitchView® IP 1020 remote access device combines analog and digital technology to provide flexible control of data center servers, and to facilitate the OA&M (operations, activation and maintenance) of remote branch offices where trained operators may be unavailable. The remote access device provides our customers with a significant reduction of cable volume, secure remote access and flexible server management from anywhere at anytime.

The SwitchView IP 1020 device is a keyboard, video and mouse (KVM) remote access device configurable for analog (local) or digital (remote) connectivity. Video resolutions up to 1280 x 1024 are supported for remote users. Enhanced video quality of up to 1600 x 1200 is available to local users via the video port.

The IP-based SwitchView IP 1020 remote access device gives you flexible target device management control from anywhere in the world.

Accessing a remote access device via network connection

No special software or drivers are required on the attached, or client, computers. Users access the SwitchView IP 1020 remote access device and an attached system via the Ethernet from a client computer, such as a PC. Clients can be located anywhere a valid network connection exists. Both IPv4 (default) or IPv6 modes are supported.

Simple access to a target device

When a user selects the target device, the video of the selected target device is displayed in a Video Viewer window.

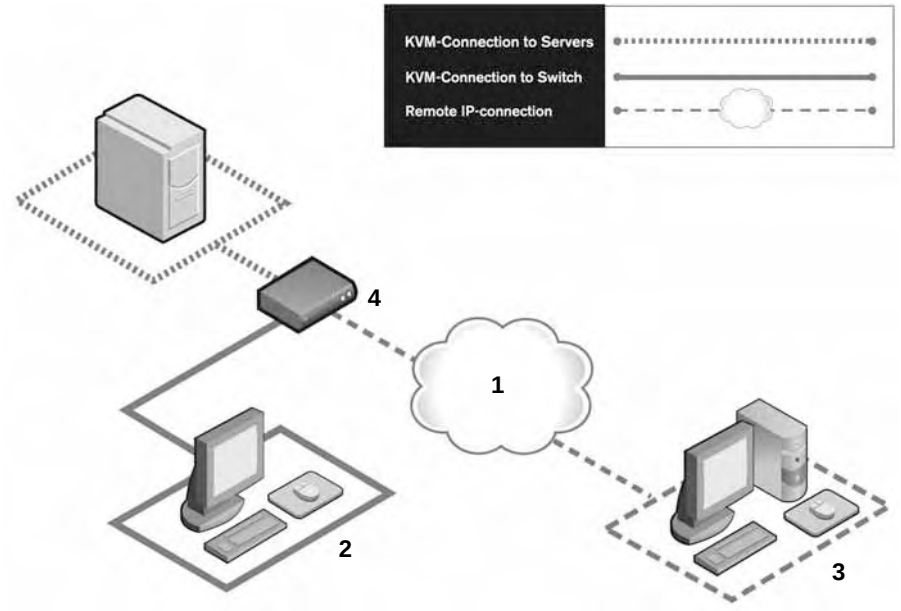

Figure 1.1: Example SwitchView IP 1020 Remote Access Device Configuration

Table 1.1: Descriptions for Figure 1.1

Number	Description
1	Ethernet
2	Analog User
3	Digital User (Computer with Internet browser)
4	SwitchView IP 1020 Remote Access Device

CHAPTER 2

Installation

SwitchView IP 1020 Remote Access Device Connectivity

The SwitchView IP 1020 remote access device transmits keyboard, video and mouse (KVM) information between operators and a target device attached to the remote access device over a network using an Ethernet connection.

The SwitchView IP 1020 remote access device uses TCP/IP for communication over Ethernet. You can access and control your target device with GUI-based simplicity using the built-in web server.

Installation Overview

The general procedure for setting up and installing a SwitchView IP 1020 remote access device is as follows:

- Unpack the switch and verify that all components are present and in good condition.
- Make all hardware connections between the power source, remote access device, target device and the Ethernet connection.
- Turn on the power and verify that all connections are working.
- Make the appropriate mouse setting adjustments.

Figure 2.1 illustrates a basic configuration for the SwitchView IP 1020 remote access device, using the SwitchView IP 1020 model for the example. Descriptions follow in Table 2.1.

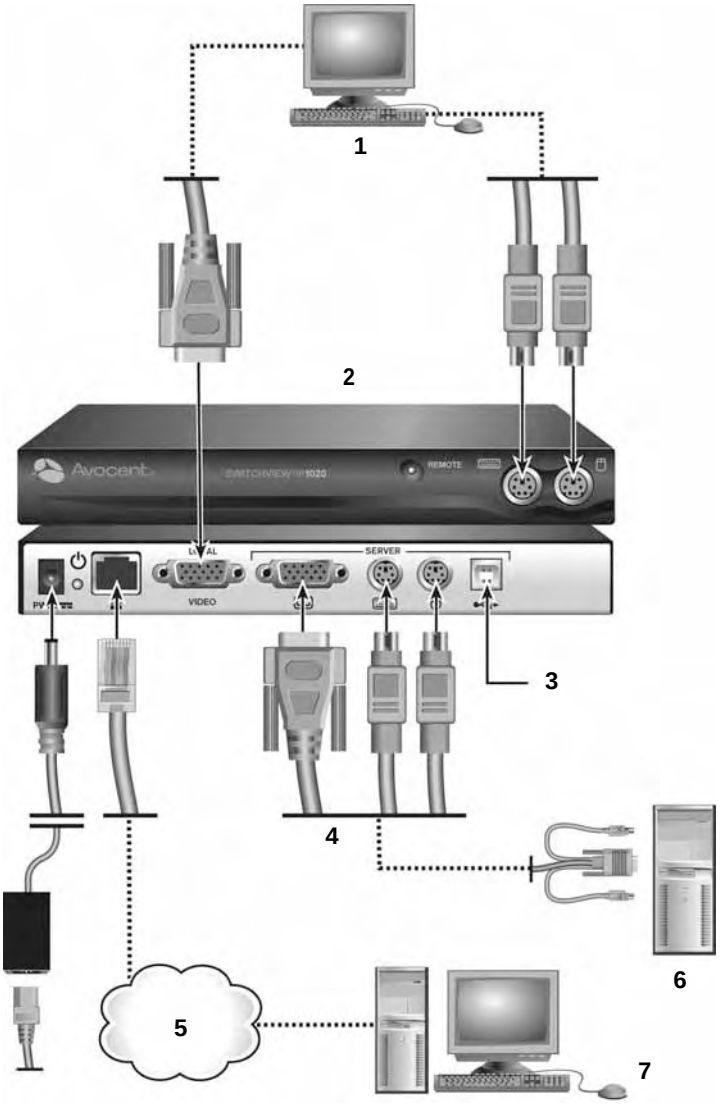

Figure 2.1: Basic SwitchView IP 1020 Remote Access Device Configuration

Table 2.1: Descriptions for Figure 2.1

Number	Description	Number	Description
1	Local User	**5**	Ethernet
2	SwitchView IP 1020 Remote Access Device	6	Server
3	Optional USB Port	**7**	Remote User
4	CPS2-6A Cable		

Getting started

Before installing your SwitchView IP 1020 remote access device, refer to the following lists to ensure you have all items that shipped with the SwitchView IP 1020 remote access device, as well as other items necessary for proper installation.

Supplied with the SwitchView IP 1020 remote access device

- Power adaptor
- Power cord
- Avocent CPS2-6A cable
- SwitchView IP 1020 Remote Access Device Quick Installation Guide

Additional items needed

- One CAT5 patch cable for network connectivity (4 pair UTP)

Setting up your network

The SwitchView IP 1020 remote access device system uses IP addresses to uniquely identify the switch and the target device. The SwitchView IP 1020 remote access device family supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Avocent recommends that IP addresses be reserved for each SwitchView IP 1020 remote access device and that they remain static while the switches are connected to the network.

Connecting the Remote Access Device Hardware

To connect and power your SwitchView IP 1020 remote access device:

1. Power down the target server that will be attached to your SwitchView IP 1020 remote access device. Locate the power adaptor and cord that came with your remote access device. Plug the barrel connector into the back panel of the SwitchView IP 1020 device, the AC power cord into the adaptor block and the AC connector into an appropriate AC wall outlet.

WARNING: The power cord is considered the main disconnect device.

2. To connect a local user, plug a VGA monitor into the port labeled LOCAL VIDEO on the back panel of the remote access device. Plug the PS/2 keyboard and mouse cables into the appropriately labeled ports located on the front of the remote access device.
3. To connect to the server, plug one end of the CPS2-6A cable into the server's VGA, keyboard and mouse ports. Plug the other end into the SERVER VGA, keyboard and mouse ports on the back panel of the SwitchView IP 1020 remote access device.

NOTE: If using USB keyboard and mouse peripherals, plug one end of a USB cable into the server and the other end into the optional USB port on the SwitchView IP 1020 device. Disconnect the PS/2 connectors of the CPS2-6A cable from the server, if applicable.

4. Plug a CAT 5 patch cable from your Ethernet network into the LAN port on the back of the SwitchView IP 1020 remote access device.
5. Power up the target device and then the SwitchView IP 1020 remote access device. After approximately one minute, the device will complete initialization and display video on the local port monitor.
6. Point your web browser to the default IP address https://192.168.1.254 to access the device.
7. Log in to the SVIP1020 Explorer window and, using the top menu bar, select *Appliance-Appliance Settings-Network.* Enter the appropriate addressing information for your network.

NOTE: The default username is Admin with no password.

SwitchView IP 1020 remote access device LEDs

The front panel of the SwitchView IP 1020 remote access device features a blue LED that indicates remote connection. On the back panel of the device, a green LED indicates power. If the power LED blinks continuously, the device is in recovery mode.

Also, on the back panel of the device, the two LEDs for the LAN connector do the following:

- Illuminates green when a valid connection to the network is established and blinks when there is activity on the port

Illuminates amber to indicate that you are communicating at the 100 Mbps rate when using an Ethernet connection

Adjusting Mouse Settings on Target Devices

Before a computer connected to the SwitchView IP 1020 remote access device can be used for remote user control, you must set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003), use the default PS/2 mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to “none” for all user accounts accessing the target computer with the SwitchView IP 1020 remote access device. Mouse acceleration must also be set to “none” on every remote system. Special cursors should not be used and cursor visibility options, such as pointer trails, **Ctrl** key cursor location animations, cursor shadowing and cursor hiding, should also be turned off.

CHAPTER 3

Web Interface Operations

On-Board Web Interface

The SwitchView IP 1020 remote access device provides an on-board web interface to manage remote access. The remote access device on-board web interface provides secure “point-and-click” web browser-based access to control any device attached to your SwitchView IP 1020 remote access device.

Table 3.1 shows which operating systems and browsers the SwitchView IP 1020 remote access device on-board web interface supports.

Table 3.1: On-Board Web Interface Supported Operating Systems and Browsers

	Browser		
Operating System	**Microsoft® Internet Explorer version 6.0 SP1 and later**	**Mozilla version 1.7.3 and later**	**Firefox version 1.0 and later**
Windows 2000 Workstation or Server with Service Pack 2	Yes	Yes	Yes
Windows Server 2003 Standard, Enterprise or Web Edition	Yes	Yes	Yes
Windows XP Home Edition or Professional	Yes	Yes	Yes
Red Hat Enterprise Linux 3 and 4	No	Yes	Yes
Sun Solaris 9 and 10	No	Yes	Yes
Novell SUSE® Linux Enterprise 9 and 10	No	Yes	Yes
Fedora Core 4 and 5	No	Yes	Yes
Mac OS X Tiger (10.4+)	No	No	Yes

NOTE: Mac OS X requires Firefox 1.5 or later.

Avocent recommends that the browser be kept up-to-date with the latest version.

A Video Viewer window allows you to control the keyboard, monitor and mouse functions of individual target devices connected to the SwitchView IP 1020 remote access device in real time. You may also use predefined global macros to perform actions within the Video Viewer window. For instructions on how to use the Video Viewer, see Chapter 4. Once the switch has been installed and configured as described in Chapter 2 and you have set the IP address, you are ready to begin regular operation.

Logging into the SwitchView IP 1020 remote access device

NOTE: The SwitchView IP 1020 remote access device boots to the following static IP address, gateway and netmask:
IP address: 192.168.1.254
Gateway: 192.168.1.1
Netmask: 255.255.255.0

Before you can begin a KVM session, you must first login to the SwitchView IP 1020 remote access device on-board web interface.

To log into the SwitchView IP 1020 remote access device on-board web interface:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the SwitchView IP 1020 remote access device you wish to access. Use https://xxx.xx.xx.xx or https://hostname as the format.
3. When the browser makes contact with the switch, enter your username and password, then click *Login*. The SwitchView IP 1020 Explorer Window will appear.

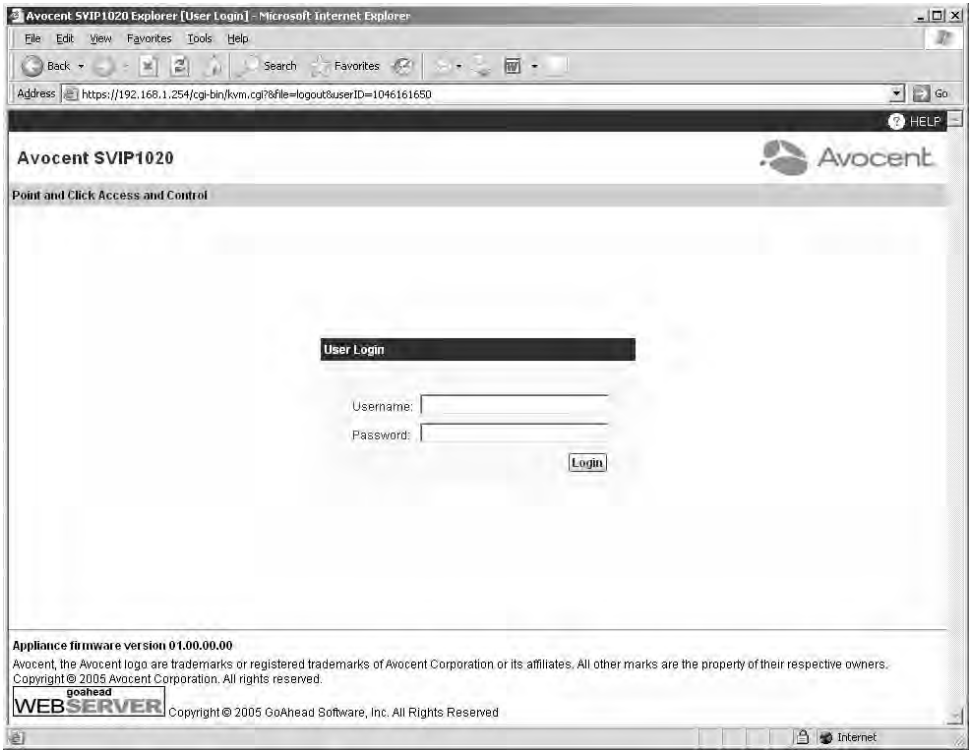
Avocent SVIP1020 Explorer [User Login] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.254/cgi-bin/kvm.cgi?&file=logout&userID=1046161650
Go
HELP
Avocent SVIP1020
Avocent
Point and Click Access and Control
User Login
Username:
Password:
Login
Appliance firmware version 01.00.00.00
Avocent, the Avocent logo are trademarks or registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.
Copyright © 2005 Avocent Corporation. All rights reserved.
goahead
WEBSERVER
Copyright © 2005 GoAhead Software, Inc. All Rights Reserved
Internet

Figure 3.1: SVIP 1020 Explorer (User Login) Screen

NOTE: The default username is Admin with no password.

The SwitchView IP 1020 Explorer Window

When a user has been logged in and authenticated, the Avocent SwitchView IP 1020 Explorer window appears. From the SwitchView IP 1020 Explorer window, users may view, access and manage their SwitchView IP 1020 remote access device. The window may also be used to specify system settings and change profile settings.

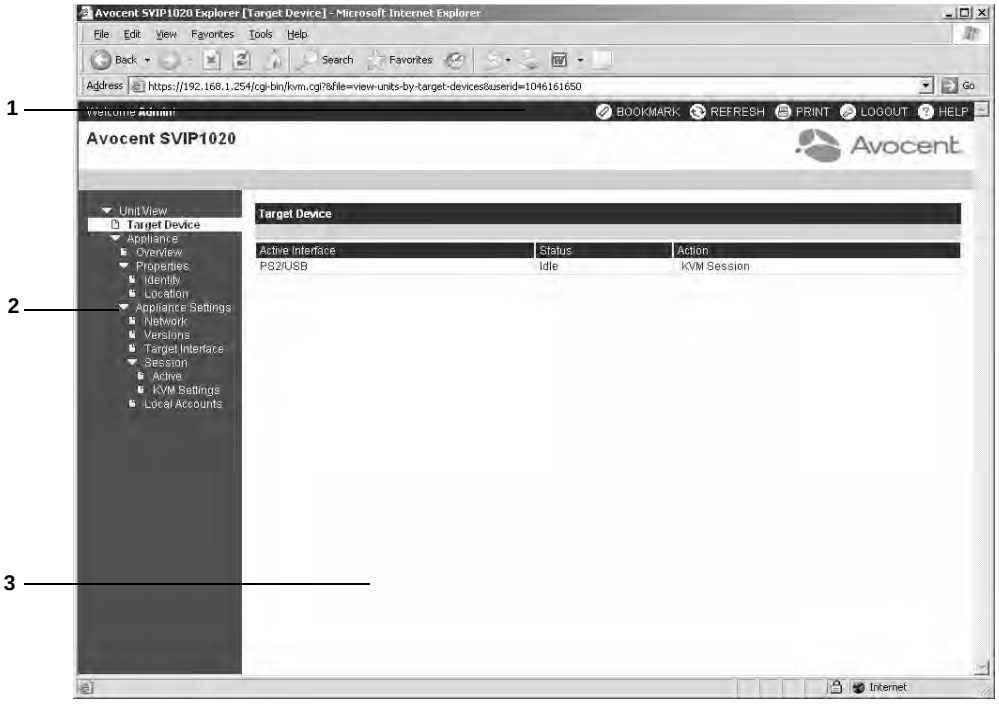

Figure 3.2: Avocent SwitchView IP 1020 Explorer Window

Table 3.2: Descriptions for Figure 3.2

Number	Description
1	Top option bar: Use the top option bar to bookmark a SwitchView IP 1020 remote access device on-board web interface window, refresh the display of a SwitchView IP 1020 remote access device on-board web interface window, print a web page, log out of a software session or access the Avocent Technical Support help page. The name of the logged in user appears on the left side of the top option bar.
2	Side navigation bar: Use the side navigation bar to display the system information you wish to display or edit, which displays in the content area. The side navigation bar also contains icons in the top left corner which, when clicked, expand or collapse all nodes.
3	Content area: Use the content area to display or make changes to the SwitchView IP 1020 remote access device on-board web interface system.

Using the side navigation bar

You can use the side navigation bar to display windows in which you can specify settings or perform operations. Clicking on a link that does not contain an arrow will display its corresponding window.

Using the top option bar

Bookmarking a window

The SwitchView IP 1020 Explorer window contains a bookmark icon and text in the top option bar. Bookmarking a window will add a link to the window in the Favorites drop-down menu. You may select the link at any time to quickly access the bookmarked window.

If you bookmark a window and information related to the window changes, this new information will appear in the window when you next display the bookmarked window.

If you click *BOOKMARK* or the bookmark icon after the SwitchView IP 1020 remote access device on-board web interface session has timed out, the User Login window will open and you must log in again.

To bookmark a window:

1. In the top option bar, click *BOOKMARK* or the bookmark icon. The Add Favorite dialog box will appear.
2. If you wish, type a name for the window. You may also click the *Create in* button to create or specify a folder in which to place the window.
3. Click *OK* to close the Add Favorite dialog box.

Printing a window

All SwitchView IP 1020 remote access device on-board web interface windows contain a print icon in the top option bar.

To print a SwitchView IP 1020 remote access device on-board web interface window:

1. In the top option bar, click *PRINT* or the print icon. The Print dialog box will appear.
2. Specify the options you wish to use for printing the SwitchView IP 1020 remote access device on-board web interface window.
3. Click *Print* to print the SwitchView IP 1020 remote access device on-board web interface window and close the Print dialog box.

Refreshing a window

The SwitchView IP 1020 Explorer window may be refreshed at any time by clicking *REFRESH* or the refresh icon in the top option bar.

Logging out

A user may log out at any time by clicking the logout icon in the top option bar.

Managing local accounts

The remote access device web interface provides local and login security through Administrator-defined user accounts. By selecting *Local Accounts* on the side menu bar, Administrators may add and delete users, define user preemption and access levels and change passwords.

User access levels

Accounts have two access levels: user and administrator. Most switch management tasks can only be performed by persons with administrator level access.

Preemption levels

The preemption level of users determine whether they may disconnect another user's serial or video (KVM) session with a target device.

Remote access device web interface administrators may specify the preemption level for user accounts when an account is created. The preemption level may be changed later.

Preemption levels range from 1-4, with 4 being the highest level. For example, a user with a preemption level of 4 may preempt other level 4 users, as well as those with a level 1, 2 or 3 setting.

To add a new user account (Administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the *Add* button.
3. Enter the name and password of the new user in the blanks provided.
4. Select the preemption and access levels for the new user.
5. Click the *Save* button to complete the process.

To delete a user account (Administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the box to the left of each account that you wish to delete, then click the delete button.

To edit a user account (Administrator or active user only):

1. On the side menu bar, select local accounts. The current user list will be displayed.
2. Click the name of the user you wish to edit. A user profile will appear.
3. Edit the user account as needed, then click *Save*.

Managing device properties

Viewing and changing appliance configuration information

The SwitchView IP 1020 remote access device can report most device properties directly through the remote access device web browser.

NOTE: Users can view all appliance information, but only Administrators can change settings.

Table 3.3: Viewing Appliance Information

To do this:	Select this:
Display the unit's name or type	*Appliance - Overview*
Display a list of available target devices, their type and status	*Target Devices*
Enter, change or display the unit's IP version, network address, gateway address, subnet mask, MAC address, LAN speed, DHCP enable status or ICMP ping reply status	*Appliance - Appliance Settings - Network* **NOTE:** If DHCP is set to Enabled before changing the IP mode to either IPv4 or IPv6, the user should also verify that the DHCP server has a predetermined IP address associated with the MAC address of the remote access device.
Display the unit's current firmware revision for application, boot and Video FPGA	*Appliance - Appliance Settings - Versions*
Display a list of active KVM sessions and their duration	*Appliance - Appliance Settings - Sessions - Active*
View the unit's part number, serial number and EID number	*Appliance - Properties - Identity*
Enter or display the unit's Site, Department and Location	*Appliance - Properties - Location*
Enable the inactivity timeout	*Appliance - Appliance Settings - Sessions - KVM settings* Then, click the *Enable Inactivity timeout* box.
Change the unit encryption level	*Appliance - Appliance Settings - Sessions - KVM settings* Then select the level of encryption desired for keyboard/ mouse signals and then video signals.

Configuring LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy and integrity.

If individual user accounts are stored on an LDAP-enabled directory service, such as Active Directory, you can use the directory service to authenticate users. The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the OBWI let you configure your authentication configuration parameters. The software sends the username, password and other information to the appliance, which then determines whether the user has permission to view or change configuration parameters for the appliance in the OBWI.

NOTE: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values may cause LDAP authentication server communication errors.

LDAP Overview parameters

On the LDAP Overview page in the OBWI, you can configure the LDAP authentication priority and the parameters that define LDAP server connection information.

LDAP authentication priority

In the LDAP Priority section of the LDAP Overview page, you can disable LDAP, or you can set the authentication priority by choosing whether local authentication or LDAP authentication should happen first.

To configure LDAP authentication priority parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.*
2. Select either *LDAP Disabled*, *LDAP before Local* or *LDAP after Local* for the LDAP Priority.
3. Click *Save*.

LDAP servers

The Address fields specify the host names or IP addresses of the primary and secondary LDAP servers. The second LDAP server is optional.

The Port fields specify the User Datagram Protocol (UDP) port numbers that communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP (LDAPS). The default Port ID is automatically entered by the software when an access type is specified.

The Access Type radio buttons specify how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords and other information sent between an appliance and LDAP server are sent as non-secure clear text. Use LDAPS for secure encrypted communication between an appliance and LDAP server.

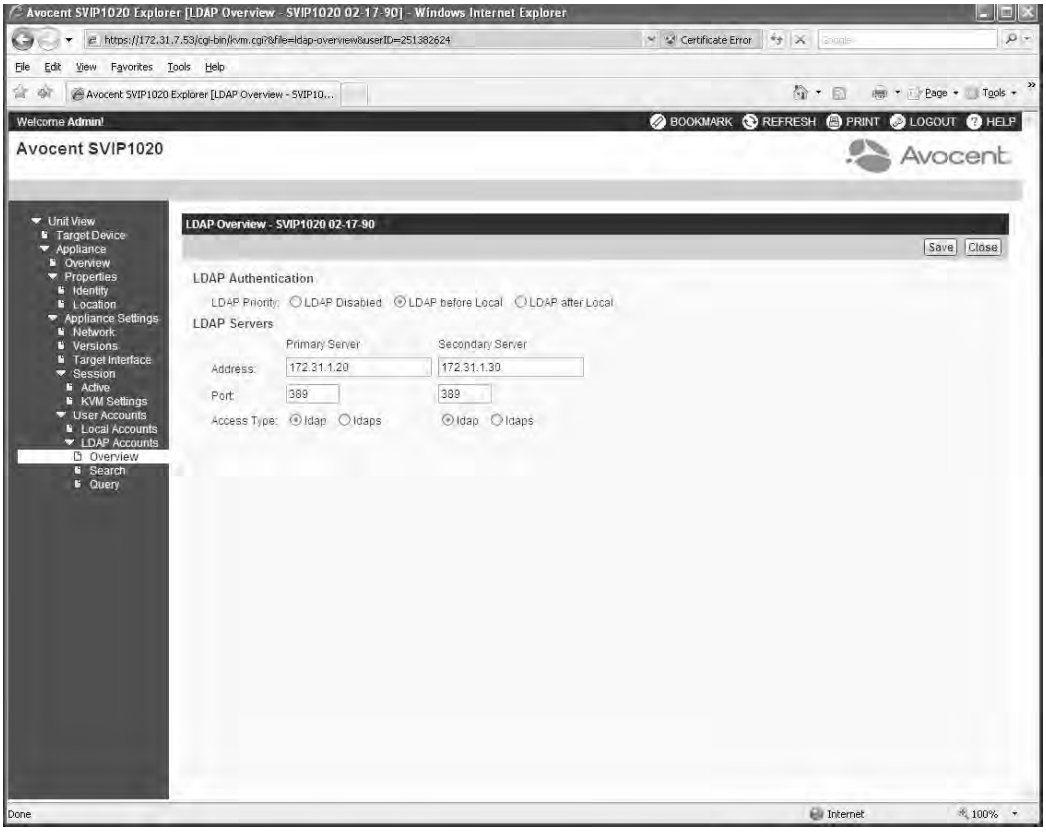

Figure 3.3: LDAP Overview Page in the OBWI

To configure LDAP server parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.*
2. Identify the primary and secondary server address, port and access type in the appropriate fields or radio buttons.
3. Click *Save*.

LDAP Search parameters

On the LDAP Search page, you can configure the parameters used when searching for LDAP directory service users.

Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the Query page. The default values are cn=Administrator, cn=Users, dc=yourDomainName and dc=com and may be modified. For

example, to define an administrator Distinguished Name (DN) for test.view.com, type **cn=Administrator, cn=Users, dc=test, dc=view,** and **dc=com.** This Search DN field is a required field unless the directory service has been configured to enable anonymous search, which is not the default. Each Search DN value must be separated by a comma.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

Use the Search Base field to define a starting point from which LDAP searches begin. The modifiable default values are dc=yourDomainName and dc=com. For example, to define a search base for test.com, type **dc=test, dc=com**. Each Search Base value must be separated by a comma.

The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form <name>=<%1>. The default value is sAMAccountName=%1, which is correct for use with Active Directory. This field is required for LDAP searches.

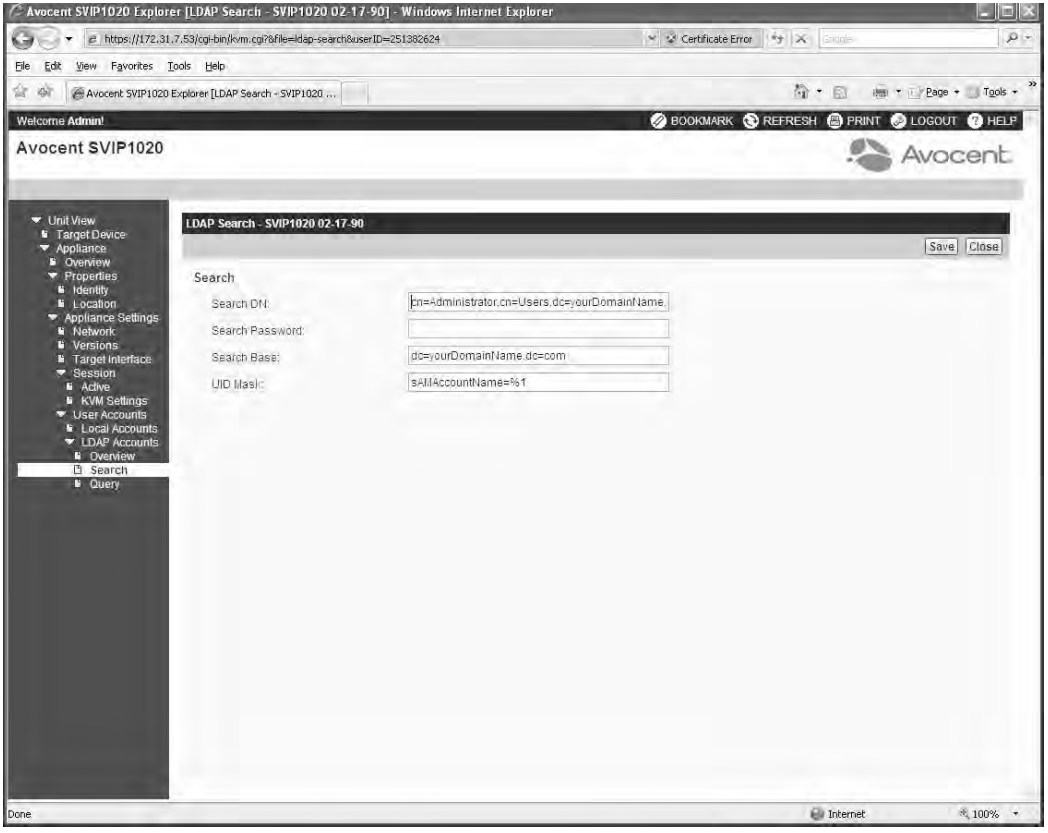

Figure 3.4: LDAP Search Page in the OBWI

To configure LDAP search parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Search*.
2. Enter the appropriate information in the Search DN, Search Password, Search Base and UID Mask fields.
3. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

LDAP Query parameters

On the LDAP Query page, you can configure the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators attempting to access the appliance itself. Query Mode (Target Device) is used to authenticate users that are attempting to access attached target devices. Additionally, each type of query has three modes that utilize certain types of information to determine whether or not a VCS user has access to an appliance or connected target devices. See *Appliance and Target Device Query Modes* on page 21 for detailed information on each mode.

You can configure the following settings on the LDAP Query page:

- The Query Mode (Appliance) parameters determine whether or not a user has access to the appliance.
- The Query Mode (Target Device) parameters determine whether or not a user has user access to target devices connected to an appliance. The user does not have access to the appliance.
- The Group Container, Group Container Mask and Target Mask fields are only used for group query modes and are required when performing an appliance or device query.
- The Group Container field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects. Group objects are Active Directory objects that can contain users, computers, contacts and other groups. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object. For example, if the Notes property in the group object is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query page should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.
- The Notes property is used to implement the access control attribute. The value of the Notes property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the info attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by

selecting *Start - Programs - Administrative Tools -Active Directory Users and Computers*. This tool is used to create, configure and delete objects such as users, computers and groups.

- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is “ou=%1”.
- The Target Mask field defines a search filter for the target device. The default value is “cn=%1”.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to Attribute. The default value is info.

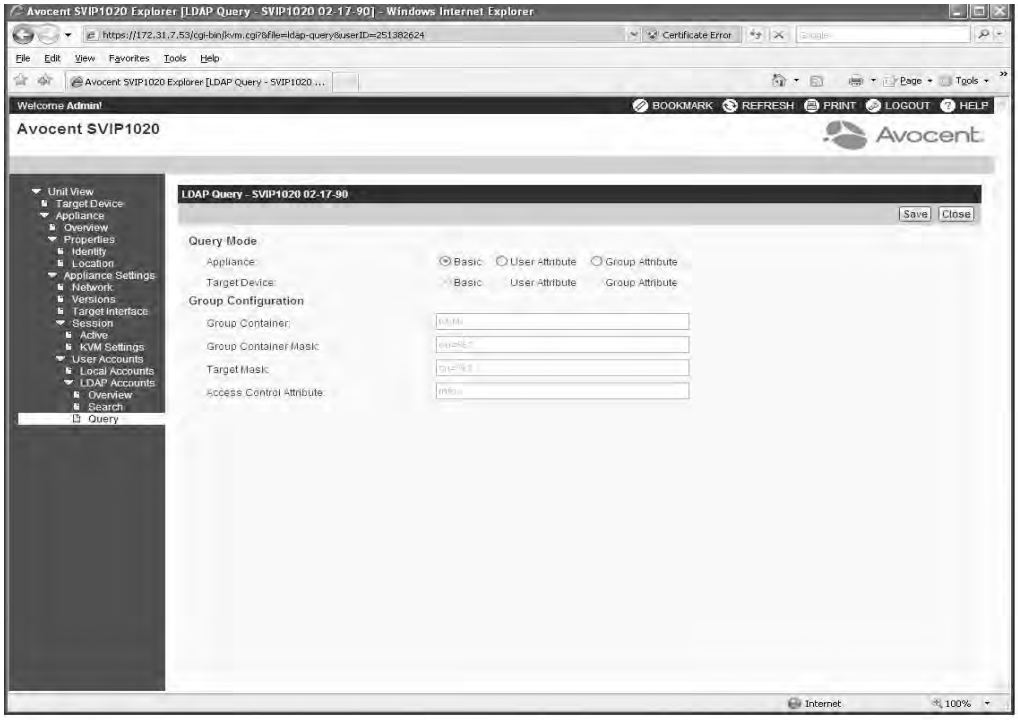

Figure 3.5: LDAP Query Page in the OBWI

To configure LDAP query parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Query.*
2. Select either *Basic*, *User Attribute* or *Group Attribute* for the Appliance Query Mode and the Target Device Query Mode.
3. Enter the appropriate information in the Group Container, Group Container Mask, Target Mask and Access Control Attribute fields.
4. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

Appliance and Target Device Query Modes

One of three different modes can each be used for Query Mode (Appliance) and Query Mode (Target Device):

- Basic – A username and password query for the user is made to the directory service. If they are verified, the user is given administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).
- User Attribute – A username, password and Access Control Attribute query for the appliance user is made to the directory service. The Access Control Attribute is read from the user object (the user account) in Active Directory.

  If the KVM Appliance Admin value is found, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device). If the KVM User Admin value is found, the user is given User administrator access to the appliance and attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).

  The following are examples showing how the KVM Appliance Admin and KVM User Admin attribute modes are defined in Active Directory for a user named John Smith, stored in the ADUC. You can access the ADUC by selecting *Start - Programs - Administrative Tools - Active Directory Users and Computers*.

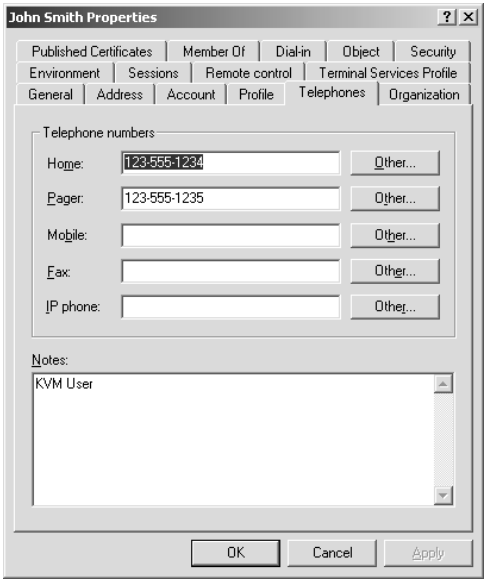

Figure 3.6: Active Directory - KVM User

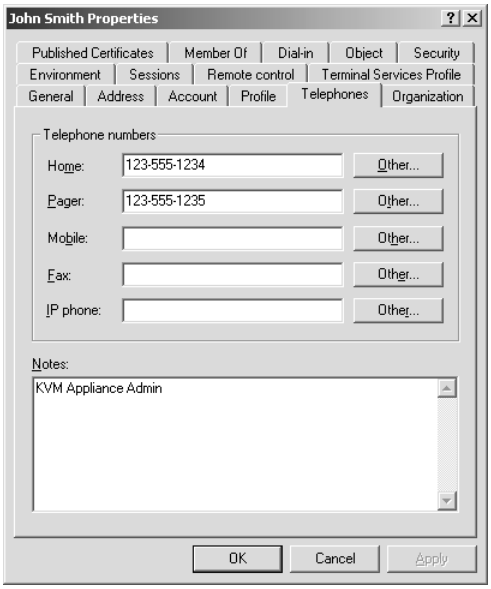

Figure 3.7: Active Directory - KVM Appliance Admin

- Group Attribute – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance), or for a selected target device when using Query Mode (Target Device). If a group is found containing the user and the appliance name, the user is given access to the appliance or attached target devices, depending on the group contents, when using Query Mode (Appliance). If a group is found containing the user and target device IDs, the user is given access to the selected target device connected to the appliance when using Query Mode (Target Device).

  Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you may have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group may contain a member named Domestic, which is a group, and so on.

  The following is an example of groups defined in Active Directory.

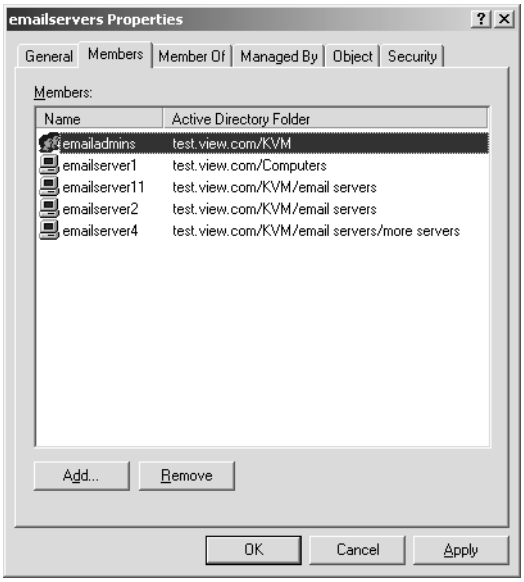

Figure 3.8: Active Directory - Define Groups

Setting up Active Directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the user.

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create an object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview screen of the OBWI), or identical to the attached target devices for querying target devices. The name must match exactly, including case.
5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview screen of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.

NOTE: The factory default name in earlier versions contains a space that must be removed by editing the switching system name in the Appliance Overview screen of the OBWI.

6. Create one or more groups under the group container organizational unit.
7. Add the usernames and target device and appliance objects to the groups you created in step 5.

Specify the value of any attribute being used to implement the access control attribute. For example, if you are using info as the attribute in the Access Control Attribute field and using the Notes property in the group object to implement the access control attribute, the value of the Notes attribute in Active Directory may be set to one of the three available access levels (KVM User, KVM User Admin or KVM Appliance Admin) for the group object. The members of the group may then access the appliances and target devices at the specified access level.

Rebooting the appliance

Periodically, such as after an upgrade, you may need to reboot the SwitchView IP 1020 remote access device.

To reboot the SwitchView IP 1020 remote access device remotely:

1. From the side navigation bar, select *Appliance - Overview.*
2. When the appliance overview window appears, click *Tools - Reboot Appliance*.

Managing local accounts

The SwitchView IP 1020 remote access device on-board web interface provides local and login security through administrator-defined user accounts. By selecting *Local Accounts* on the side menu bar, administrators may add and delete users, define user preemption and access levels and change passwords.

Access levels

When a user account is added to the on-board web interface, the user may be assigned to any of the following access levels:

- Appliance administrators
- User administrators
- Users

Table 3.4: Allowed Operations by Access Level

	Access Level		
Operation	**Appliance Administrator**	**User Administrator**	**Users**
Configure on-board web interface system-level settings	Yes	No	No
Configure access rights	Yes	Yes	No
Add, change and delete user accounts	Yes, for all access levels	Yes, for users and user administrators only	No
Change your own password	Yes	Yes	Yes
Access target device	Yes, all target devices	Yes, all target devices	Yes, if allowed

To add a new user account (administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the *Add* button.
3. Enter the name and password of the new user in the blanks provided.
4. Select the preemption and access levels for the new user.
5. Click the *Save* button to complete the process.

To delete a user account (administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the box to the left of each account that you wish to delete, then click the *Delete* button.

To edit a user account (administrator or active user only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the name of the user you wish to edit. A user profile will appear.
3. Edit the user account as needed, then click *Save*.

Preemption levels

The preemption level of users determines whether they may disconnect another user's serial or video (KVM) session with a target device.

SwitchView IP 1020 remote access device on-board web interface administrators may specify the preemption level for user accounts when an account is created. Preemption levels range from 1-4,

with 4 being the highest level. For example, a user with a preemption level of 4 may preempt other level 4 users, as well as those with a level 1, 2 or 3 setting.

CHAPTER 4

The Video Viewer

The Video Viewer Window

The Video Viewer is used to conduct a KVM session with the target device attached to a SwitchView IP 1020 remote access device. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window containing both the local and the target device cursor. The Video Viewer window supports either a 3- or 5-button mouse.

The SwitchView IP 1020 remote access device on-board web interface software uses a Java-based program to display the Video Viewer window. The SwitchView IP 1020 remote access device OBWI automatically downloads and installs the Video Viewer the first time it is opened.

NOTE: The SwitchView IP 1020 remote access device on-board web interface does not install the Java Resource Engine (JRE). The JRE is available as a free download from http://www.sun.com for PC users and from http://www.apple.com for Mac users. When in IPv4 mode, Java 1.5 or later is required. When in IPv6 mode, Java 1.6 or later is required. Currently, MAC operating systems only support Java 1.5, so users with MAC operating systems cannot yet operate in IPv6 mode.

NOTE: The SwitchView IP 1020 remote access device on-board web interface uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory:

- An 8-bit color setting on the client PC requires 1.4 MB of memory per Video Viewer window.
- A 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB.

If the device you are attempting to access is currently being viewed by another user, you will be prompted to preempt the other users if your preemption level is equal to or greater than theirs. An appliance administrator can also disconnect an active user via the Active Session page.

Launching a KVM Session

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as Grayscale) use less network bandwidth than others (such as Best Color), changing the color settings can increase video performance. For optimal video performance over a slower network connection, Avocent recommends a color setting such as Grayscale/Best Compression or Low Color/High Compression. See *1024 x 768 768 x 576 960 x 720 704 x 528 896 x 672 640 x 480 832 x 624* on page 32 for more information.

NOTE: If a user connects to a target device with a higher screen resolution than the local computer, the Video Viewer window will display a portion of the target device screen, with scroll bars for viewing the remainder of the screen. The user may view the entire screen by adjusting the resolution on the target device, the local computer or both.

To launch a KVM session from the SwitchView IP 1020 Explorer window:

1. Click on a device listed on the Target Devices screen to open the unit overview window.
2. Click the *KVM Session* link to open the Video Viewer in a new window.

Session time-out

A remote session can time-out when no activity occurs in a Session window for a specified time. The session time-out value can be configured in the Appliance KVM Session Settings window. The specified time-out value will be used the next time the switch on-board web interface is accessed.

To enable, disable or configure the session time-out:

1. In the side menu, select *Unit Views - Appliance - Appliance Settings - Sessions - KVM Settings*.
2. Select the desired setting for the *Enable Activity Timeout* box.
3. If necessary, select the time limit for the inactivity time-out.

Video Viewer Window Features

Figure 4.1 shows the Video Viewer window areas. Descriptions follow in Table 4.1.

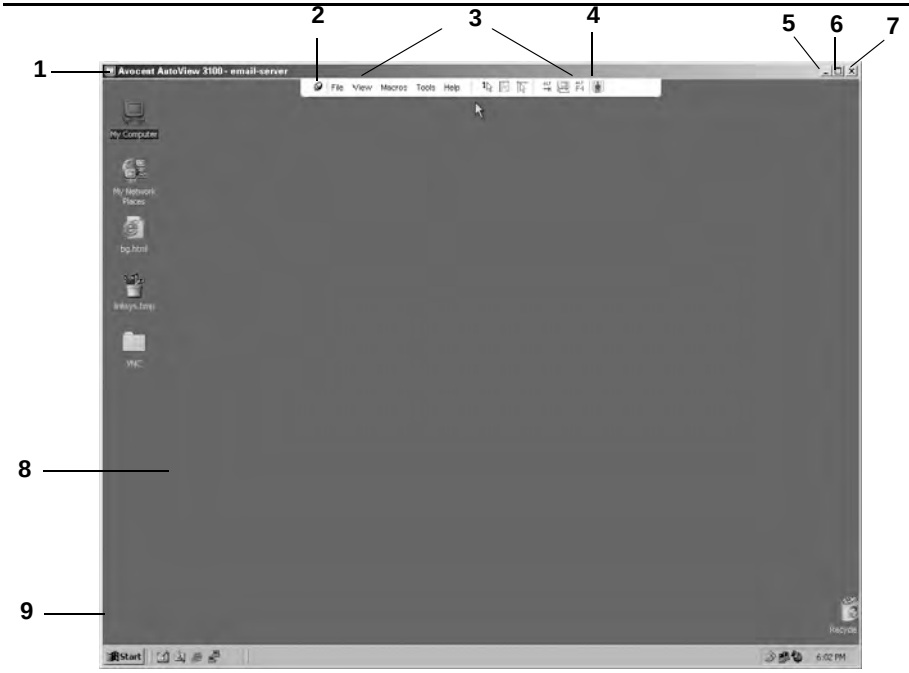

Figure 4.1: Video Viewer Window (Normal Window Mode)

Table 4.1: Descriptions for Figure 5.1

Number	Description
1	Title Bar: Displays the name of the server being viewed. When in Full Screen mode, the title bar disappears and the server name appears between the menu and toolbar.
2	Thumbtack: Locks the display of the menu and toolbar so that it is visible at all times.
3	Menu and toolbar: Enables you to access many of the features in the Video Viewer window. The menu and toolbar is in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons can be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. For more information, see *Changing the toolbar* on page 30 and *Using Macros* on page 38.
4	Macro buttons: Commonly used keyboard sequences that can be sent to the target device.
5	Minimize button: Minimizes the display of the Video Viewer window into the task bar at the bottom of the local computer.
6	Maximize button: Changes the window to Full Screen mode, which expands the accessed device desktop to fill the entire screen. Expanding the window causes the following to occur: • The title bar disappears. • The server name appears between the menu and toolbar. • The Maximize button changes to a Normal Window Mode button and appears on the toolbar. Clicking the button toggles the Video Viewer window to Normal Window mode. • The Close button appears on the toolbar.

Table 4.1: Descriptions for Figure 5.1 (Continued)

Number	Description
7	Close button: Closes the Video Viewer window. **NOTE:** The Close button may not be present for all operating systems.
8	Accessed device desktop: Interacts with your device through this window.
9	Frame: Resizes the Video Viewer window by clicking and holding on the frame.

Changing the toolbar

You can choose the amount of elapsed time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack).

To specify a toolbar hide time:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Use the arrow keys to specify the number of elapsed seconds prior to hiding the toolbar.
4. Click *OK* to save your changes and close the dialog box.

Setting the window size

NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode or to non-primary users of a shared session.

When the SwitchView IP 1020 remote access device on-board web interface is used for the first time, any open Video Viewer windows display at a resolution of 1024 x 768 until the user changes the value. Each Video Viewer window can be set to a different resolution.

The SwitchView IP 1020 remote access device on-board web interface automatically adjusts the display if the window size changes during a session as long as autoscaling is enabled. If the target device resolution changes any time during a session, the display adjusts automatically.

To change the Video Viewer window resolution:

1. Select the *View - Scaling* command.
2. Click on the desired resolution.

Adjusting the view

Using menus or task buttons in the Video Viewer window, you can do the following:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1024 x 768. If the desktop has a higher resolution, the following occurs:
  - The full-screen image is centered in the desktop, and the areas surrounding the Video Viewer window are black.
  - The menu and toolbar are locked so that they are visible at all times.
- Enable automatic, full or manual scaling of the session image:
  - With full scaling, the desktop window remains fixed and the device image scales to fit the window.
  - With automatic scaling, the desktop window is sized to match the resolution of the server being viewed.
  - With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Change the color depth of the session image.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor should align with the cursor on the remote device.

NOTE: If cursors drift out of alignment, turn off mouse acceleration in the attached device.

To refresh the screen:

Click the *Refresh Image* button in the Video Viewer window.

-or-

Select *View* - *Refresh* from the Video Viewer window menu.

The digitized video image is completely regenerated.

To enable or disable Full Screen mode:

1. To enable Full Screen mode, click the *Maximize* button.
   -or-
   Select *View* - *Full Screen* from the Video Viewer window menu.

   The desktop window disappears and only the accessed device desktop is visible. The screen resizes up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

   -or-

2. To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

To enable full or manual scaling:

To enable full scaling, select *View - Scaling* from the Video Viewer window menu. The device image scales automatically to the resolution of the server being viewed.

-or-

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu. Choose the dimension to scale the window. Available manual scaling sizes are as follows:

1024 x 768	768 x 576
960 x 720	704 x 528
896 x 672	640 x 480
832 x 624	

Adjusting color depth

The Dambrackas Video Compression® (DVC) algorithm enables users to adjust the number of viewable colors in a remote session window. You can choose to display more colors for the best fidelity or fewer colors to reduce the volume of data transferred on the network.

Video Viewer windows can be viewed using the Best Color Available (slower updates), Best Compression (fastest updates), a combination of Best Color and Best Compression or in Grayscale.

You can specify the color depths of individual ports and channels by selecting the *View - Color* command in a remote session window.

Additional video adjustment

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, users can fine-tune the video with the help of Avocent Technical Support by selecting the *Tools - Manual Video Adjust* command in the Video Viewer window menu or clicking the *Manual Video Adjust* button. This displays the Manual Video Adjust dialog box.

Users can also verify the level of packets per second required to support a static screen by observing the packet rate located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only on the advice and with the help of Avocent Technical Support.

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu.
   -or-
   Click the *Manual Video Adjust* button.

   The Manual Video Adjust dialog box appears. Figure 4.2 shows the dialog box, and descriptions follow in Table 4.2.

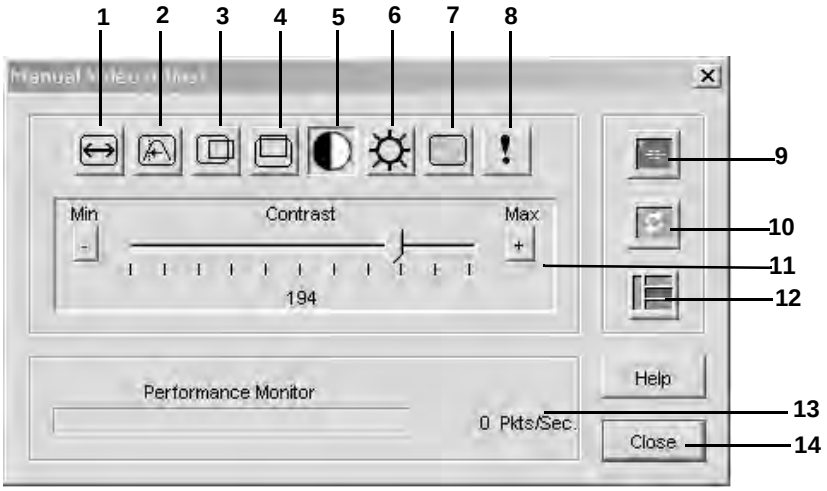

Figure 4.2: Manual Video Adjust Dialog Box

Table 4.2: Descriptions for Figure 5.2

Number	Description	Number	Description
1	Image Capture Width	**8**	Pixel Noise Threshold
2	Pixel Sampling/Fine Adjust	**9**	Automatic Video Adjustment
3	Image Capture Horizontal Position	**10**	Refresh Image
4	Image Capture Vertical Position	**11**	Adjustment bar
5	Contrast	**12**	Video Test Pattern
6	Brightness	**13**	Performance Monitor
7	Block Noise Threshold	**14**	Close button

2. Click the icon corresponding to the feature you wish to adjust.
3. Move the Contrast slider bar and then fine-tune the setting by clicking the *Min* (-) or *Max* (+) buttons to adjust the parameter for each icon pressed. The adjustments display immediately in the Video Viewer window.
4. When finished, click *Close* to exit the Manual Video Adjust dialog box.

Target video settings

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized and are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Contrast and brightness

If the image in the Video Viewer window is too dark or too light, select *Tools - Automatic Video Adjust* or click the *Automatic Video Adjust* button. This command is also available in the Video Adjustments dialog box. In most cases, this corrects video issues.

When clicking *Auto Adjust* several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually can help. Increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up, which is indicated by little dots changing in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and can improve cursor tracking.

You can modify Noise Threshold and Priority Threshold values if you are using standard video compression. You can also modify Block Noise Threshold and Pixel Noise Threshold values. You can restore default threshold values by clicking *Auto Adjust Video*.

Block Noise Threshold and Pixel Noise Threshold

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed.

- The Block Noise Threshold sets the minimum color change that occurs in a single video block. Increasing the value reduces the network bandwidth. Decreasing the value makes the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value reduces the number of low-contrast artifacts, but increases network bandwidth.

See *Adjusting the view* on page 30 for information about changing the color depth.

Automatic video adjustment

In most cases, you do not need to alter the Video Settings from the default. The system automatically adjusts and uses the optimal video parameters. The SwitchView IP 1020 remote access device on-board web interface performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You can easily adjust your video parameters to ideal settings by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box.

NOTE: You can also select *Tools - Automatic Video Adjust* from the Video Viewer window menu or click the *Automatic Video Adjust* toolbar icon to automatically adjust the video.

Refresh Image

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box completely regenerates the digitized video image.

NOTE: You can also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Video Test Pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box toggles a display of a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Adjusting mouse options

The Video Viewer window mouse options affect cursor type, Cursor mode, scaling, alignment and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

NOTE: If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor type

The Video Viewer window offers five appearance choices for the local mouse cursor. You can also choose no cursor or the default cursor.

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window turns off and only the target device mouse pointer is visible. The only mouse movements that appear are those of the target device remote cursor. Use Single Cursor mode when there is no need for a local cursor. Figure 4.3 shows both the Remote Cursor and the Local Cursor displayed in the Video Viewer window.

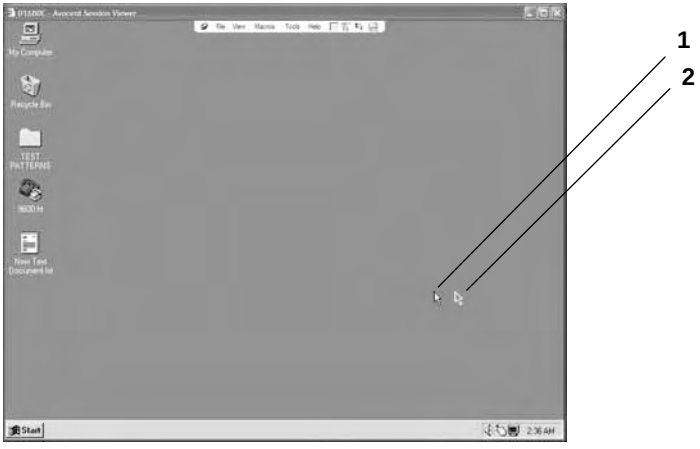

Figure 4.3: Video Viewer Window with Local and Remote Cursors Displayed

Table 4.3: Descriptions for Figure 5.3

Number	Description
1	Remote Cursor
2	Local Cursor

The Cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You can define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the client, you should avoid using those keys to restore the mouse pointer.

To enter Single Cursor mode:

Select *Tools - Single Cursor Mode* from the Video Viewer window menu.

-or-

Click the *Single Cursor Mode* button.

The local cursor does not appear and all movements are relative to the target device.

To select a key for exiting Single Cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK* to save settings.

When you enable Single Cursor mode, you can press the specified key to return to Regular Desktop mode.

To exit Single Cursor mode:

Press the key on the keyboard that is identified in the title bar.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK* to save settings.

Mouse scaling

Some earlier versions of Linux did not support adjustable mouse accelerations. For installations that must support these earlier versions, you can choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are Default (1:1), High (2:1) or Low (1:2):

- In a 1:1 scaling ratio, every mouse movement on the desktop window sends an equivalent mouse movement to the server.
- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.
- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.
   -or-
   To set custom scaling:
   a. Click the *Custom* radio button to enable the X and Y fields.
   b. Type a scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input range is 0.25-3.00.

Vendor-specific video settings

Video settings vary significantly among manufacturers. Avocent maintains an online database of optimized video settings for various video cards, particularly Sun-specific ones. This information can be obtained from Avocent's online knowledge base or by calling Avocent technical support.

Mouse alignment and synchronization

Because the SwitchView IP 1020 remote access device on-board web interface cannot get constant feedback from the mouse, there are times when the mouse on the SwitchView IP 1020 remote access device may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you can align the mouse to re-establish proper tracking.

Alignment causes the local cursor to align with the remote server's cursor. Resetting causes a simulation of a mouse and keyboard reconnect as if you had disconnected and reconnected them.

To realign the mouse:

Click the *Align Local Cursor* button in the Video Viewer window toolbar.

Using Keyboard Pass-through

Keystrokes that a user enters when using a Video Viewer window may be interpreted in two ways, depending on the Screen mode of the Video Viewer window.

- If a Video Viewer window is in Full Screen mode, all keystrokes and keyboard combinations except **Ctrl-Alt-Del** are sent to the remote server being viewed.
- If a Video Viewer window is in Regular Desktop mode, Keyboard Pass-through mode can be used to control whether the remote server or local computer recognizes certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the Session Options dialog box. When enabled, keyboard pass-through sends all keystrokes and keystroke combinations except **Ctrl-Alt-Del** to the remote server being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The **Ctrl-Alt-Delete** keyboard combination can be sent only to a remote server by using a macro.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote server regardless of the Screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK* to save setting.

Using Macros

The SwitchView IP 1020 remote access device on-board web interface comes pre-configured with macros for the Windows and the Sun platforms.

To send a macro:

Select *Macros - <desired macro>* from the Video Viewer window menu.

-or-

Select the desired macro from the buttons available on the Video Viewer menu.

Saving the View

You can save the display of a Video Viewer either to a file or to the clipboard for pasting into a word processor or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu.
   -or-
   Click the *Capture to File* button.

   The Save As dialog box appears.
2. Enter a filename and choose a location to save the file.
3. Click *Save* to save the display to a file.

To capture the Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the Video Viewer window menu.

-or-

Click the *Capture to Clipboard* button.

The image data is saved to the clipboard.

Closing a Video Viewer Window Session

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

APPENDICES

Appendix A: Flash Upgrades

The SwitchView IP 1020 remote access device Flash upgrade feature allows you to update your appliance with the latest firmware available.

After the Flash memory is reprogrammed with the upgrade, the SwitchView IP 1020 remote access device performs a soft reset, which terminates all IQ module sessions. A target device experiencing an IQ module firmware update may not display, or may display as disconnected. The target device will appear normally when the Flash update is completed.

CAUTION: Disconnecting or cycling power to the SwitchView IP 1020 device during an update may render the device inoperable and require the SwitchView IP 1020 device to be reprogrammed using the recovery procedure.

To update the SwitchView IP 1020 remote access device firmware:

1. Visit http://www.avocent.com/support and download the latest Flash firmware from Avocent. Save the Flash update file to the appropriate directory on a computer that can access the SwitchView IP 1020 remote access device.
2. If the SwitchView IP 1020 remote access device is not on, turn it on now. After approximately one minute, proceed to login.
3. Select *Firmware Management* to display the current version of your firmware on the Firmware Management menu.
4. Click the *Upgrade Firmware* button.
5. Use the browser to find the appropriate directory and filename.
6. Click the *Upgrade* button.
7. The SwitchView IP 1020 remote access device begins the Flash update process. On-screen indicators display the update progress. When the upload is complete, the SwitchView IP 1020 remote access device resets and updates the internal subsystems.
8. Once the update is complete, the login screen will appear.

NOTE: If the green LED on the back panel of the device blinks continuously, the device is in recovery mode.

To recover a Flash update:

NOTE: If you do not have a TFTP server, you can find several shareware and freeware programs on the Internet that you can download and install.

1. Visit http://www.avocent.com/support and download the latest Flash firmware from Avocent. Save the Flash update file to the appropriate directory on the TFTP server.
2. Use the server IP address 192.168.1 to set up the TFTP server.
3. Rename the downloaded file name to svip1020.fl and place it into the TFTP root directory of the TFTP server.
4. Make sure the SwitchView IP 1020 device is powered.

The recovery should start automatically.

Appendix B: Technical Specifications

Table B.1: SwitchView IP 1020 Remote Access Device Product Specifications

Server Ports	
Number	1
Type	PS/2, USB
Connectors	PS/2, USB, VGA
Sync Types	Separate horizontal and vertical
Plug and Play	DDC2B
Video Resolution	640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz (Remote port maximum)
Supported Cabling	CPS2-6A cable, 6 feet
Dimensions	
Height x Width x Depth	1.06 in x 8.19 in x 5.25 in (2.70 cm x 20.80 cm x 13.34 cm)
Weight (without cables)	1.5 lbs (0.68 kg) without cables
Network Connection	
Number	1
Type	10/100/1000 Ethernet
Connector	RJ-45
Local Port	
Number	1
Type	PS/2, VGA
Power Consumption	5 W
Operating Voltage	external 5 V DC power @ 2.0 A
AC-input Power	10.5 W maximum (120 V, 60 Hz)
AC-input Range	100 - 240 VAC

Table B.1: SwitchView IP 1020 Remote Access Device Product Specifications (Continued)

AC Frequency	50 - 60 Hz autosensing
AC-input Current Rating	0.5 A
AC-input Cable	6 ft, 2 conductor, 18 AWG
Ambient Atmospheric Condition Ratings	
Humidity	5 to 95% noncondensing (operating/storage)
Temperature	0° to 40° Celsius (32° to 104° degrees Farenheit) operating -30° to 70° Celsius (-22° to 149° Farenheit) nonoperating
Safety and EMC Standards Approvals and Markings	UL, FCC, cUL, ICES-003, CE, VCCI, MIC, C-Tick Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

Appendix C: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on a PS/2 keyboard. To enable Sun Advanced Key Emulation mode and use these keys, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key. The *Scroll Lock* LED blinks. Use the indicated keys in Table C.1 as you would use the advanced keys on a Sun keyboard.

Table C.1: Sun Key Emulation

Sun Key (US)	PS/2 Key to Enable Sun Key Emulation
Compose	Application(1)
Compose	keypad
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left)(2)	F12
Command (left)(2)	Win (GUI) left (1)
Command (right)(2)	Win (GUI) right (1)

(1)Windows 95 104-key keyboard.
(2)The Command key is the Sun Meta (diamond) key.

For example: For **Stop + A**, press and hold **Ctrl+Shift+Alt** and press Scroll Lock, then **F1 + A**.

These key combinations will work with the serial USB IQ module (if your Sun system comes with a USB port) as well as the Sun VSN and WSN IQ modules. With the exception of **F12**, these key combinations are not recognized by Microsoft Windows. Using **F12** performs a Windows key press.

When finished, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key to toggle Sun Advanced Key Emulation mode off.

Special considerations for Japanese Sun USB and Korean Sun USB keyboards (USB IQ modules only)

Japanese Sun USB and Korean Sun USB keyboards assign usage IDs for certain keys that differ from standard USB usage IDs. If USB IQ modules are attached to your Sun servers, the Han/Zen and Katakana/Hiragana keys on Japanese Sun USB keyboards and Hangul and Hanja keys on Korean Sun USB keyboards must be accessed using alternate keystrokes.

Due to these keyboard-specific differences, keyboard mapping inconsistencies may be encountered when switching between target devices using Sun VSN and WSN IQ modules and target devices using USB IQ modules. These keys function normally if your Sun servers are attached to the SwitchView IP 1020 remote access device using a VSN or WSN IQ module.

Table C.2 lists the keyboard mapping that will take place when a USB IQ module is used in this setting.

Table C.2: PS/2-to-USB Keyboard Mappings

PS/2 Keyboard	USB Usage ID	Sun USB Keyboard	Korean Sun USB Keyboard	Japanese Sun USB Keyboard
Right-Alt	0xE6	AltGraph	Hangul	Katakana/Hiragana
Windows Application	0x65	Compose	Hanja	Compose
Hangul	0x90	N/A	N/A	N/A
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35	` ~	` ~	N/A

Appendix D: Reset to Factory Defaults

To reset your SwitchView IP 1020 remote access device to the factory defaults:

1. Locate the small hole on the right side of the SwitchView IP 1020 device.
2. Insert a pin to depress the reset switch and hold for three (3) seconds.

NOTE: This will reboot the SwitchView IP 1020 remote access device, and all connections will be lost.

3. The blue LED on the front panel of the SwitchView IP 1020 device will blink twice to indicate that the device is being reprogrammed.
4. Log in to the device again once it has been reset to the factory defaults.

NOTE: The default username is Admin with no password.

Appendix E: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

Équipement d’accès à distance SwitchView® IP 1020

Guide d’installation et d’utilisation

Avocent, le logo Avocent, The Power of Being There, SwitchView, DSView, Dambrackas Video Compression et OSCAR sont des marques déposées d’Avocent Corporation ou de ses filiales. Toutes les autres marques sont la propriété exclusive de leurs détenteurs respectifs.

© 2008 Avocent Corporation. 590-538-616D

Instructions

Ce symbole est destiné à attirer votre attention sur la présence de consignes importantes liées au fonctionnement et à la maintenance (l'entretien) dans la documentation accompagnant le dispositif.

Tension dangereuse

Ce symbole est destiné à vous avertir de la présence de « tensions dangereuses » non isolées à l'intérieur de l'appareil pouvant être suffisamment élevées pour constituer un risque de choc électrique pour les individus.

Marche

Ce symbole indique que la commande principale de marche/arrêt est sur marche.

Arrêt

Ce symbole indique que la commande principale de marche/arrêt est sur arrêt.

Raccordement de protection à la terre

Ce symbole indique que l'équipement doit être relié à la terre avant d'être branché.

TABLE DES MATIÈRES

LISTE DES FIGURES ..... **vii**

LISTE DES TABLEAUX ..... **ix**

Chapitre 1 : Présentation du produit **1**

Caractéristiques et avantages *1*

Accès à un équipement d'accès à distance via une connexion réseau *1*

Accès simple à tout équipement cible *1*

Chapitre 2 : Installation **3**

Connectivité de l'équipement d'accès à distance SwitchView IP 1020 ..... *3*

Installation *3*

Démarrage *5*

Configuration de votre réseau *5*

Connexion du matériel de l'équipement d'accès à distance *6*

Voyants du SwitchView IP 1020 ..... *7*

Réglage des paramètres de la souris sur les équipements cibles *7*

Chapitre 3 : Utilisation de l'interface Web **9**

Interface Web intégrée *9*

Connexion à l'équipement d'accès à distance SwitchView IP 1020 ..... *10*

Fenêtre SwitchView IP 1020 Explorer (Explorateur du SwitchView IP 1020) *11*

Utilisation de la barre de navigation latérale *12*

Utilisation de la barre d'options supérieure *13*

Gestion des comptes locaux *14*

Gestion des propriétés des équipements *15*

Configuration LDAP *16*

Paramètres de la page Vue d'ensemble LDAP *16*

Paramètres de la page LDAP Search (Recherche LDAP) *18*

Paramètres de la page LDAP Query (Requête LDAP) *20*

Modes de requête matériel et équipement cible *22*

Configuration d'Active Directory pour la transmission de requêtes *24*

Redémarrage du matériel *25*

Gestion des comptes locaux *26*

Niveaux d'accès *26*
Niveaux de préemption *27*

Chapitre 4 : Visualiseur vidéo 29

Fenêtre du visualiseur vidéo *29*
Lancement d'une session KVM *30*
Expiration de session *30*
Caractéristiques de la fenêtre du visualiseur vidéo *30*
Modification de la barre d'outils *32*
Réglage de la taille de la fenêtre *32*
Réglage de l'affichage *33*
Réglage de la profondeur d'échantillonnage *34*
Réglage vidéo supplémentaire *35*
Paramètres vidéo cibles *36*
Contraste et brillance *36*
Seuils de détection *37*
Seuil de bruit des blocs et des pixels *37*
Réglage vidéo automatique *37*
Actualiser image *37*
Modèle d'essai vidéo *38*
Réglage des options de la souris *38*
Type de curseur *38*
Mise à l'échelle de la souris *40*
Paramètres vidéo spécifiques aux fournisseurs *40*
Alignement et synchronisation de la souris *41*
Transmission des frappes au clavier *41*
Utilisation de macros *42*
Enregistrement de l'image *42*
Fermeture d'une session du visualiseur vidéo *42*

Annexes 43

Annexe A : Mises à jour Flash *43*
Annexe B : Spécifications techniques *45*
Annexe C : Émulation des touches avancées du clavier Sun *47*
Annexe D : Réinitialisation de l'équipement aux valeurs par défaut *49*

Annexe E : Assistance technique *50*

LISTE DES FIGURES

Figure 1.1 : Exemple de configuration d'un équipement d'accès à distance SwitchView IP 1020 2
Figure 2.1 : Exemple de configuration de base d'un équipement d'accès à distance SwitchView IP 1020 4
Figure 3.1 : Écran User Login (Connexion de l'utilisateur) de l'explorateur du SVIP 1020 11
Figure 3.2 : Fenêtre de l'explorateur du SwitchView IP 1020 d'Avocent 12
Figure 3.3 : Page LDAP Overview de l'interface Web intégrée 17
Figure 3.4 : Page LDAP Search de l'interface Web intégrée 19
Figure 3.5 : Page LDAP Query de l'interface Web intégrée 21
Figure 3.6 : Utilisateur KVM dans Active Directory 23
Figure 3.7 : Administrateur de matériel KVM dans Active Directory 23
Figure 3.8 : Groupes définis dans Active Directory 24
Figure 4.1 : Fenêtre du visualiseur vidéo (mode d'affichage normal) 31
Figure 4.2 : Boîte de dialogue Manual Video Adjust 35
Figure 4.3 : Curseurs local et distant affichés dans la fenêtre du visualiseur vidéo 38

LISTE DES TABLEAUX

Tableau 1.1 : Descriptions de la Figure 1.1 ..... *2*

Tableau 2.1 : Description de la Figure 2.1 ..... *5*

Tableau 3.1 : Systèmes d'exploitation et navigateurs pris en charge par l'interface Web intégrée *9*

Tableau 3.2 : Description de la Figure 3.2 ..... *12*

Tableau 3.3 : Affichage des informations relatives au matériel *15*

Tableau 3.4 : Opérations autorisées par niveau d'accès *26*

Tableau 4.1 : Description de la Figure 5.1 ..... *31*

Tableau 4.2 : Descriptions de la Figure 5.2 ..... *36*

Tableau 4.3 : Descriptions de la Figure 5.3 ..... *39*

Tableau B.1 : Spécifications produit de l'équipement d'accès à distance SwitchView IP 1020 ..... *45*

Tableau C.1 : Émulation des touches du clavier Sun *47*

Tableau C.2 : Mappages de touches PS/2-USB *48*

CHAPITRE 1

Présentation du produit

Caractéristiques et avantages

L'équipement d'accès à distance SwitchView® IP 1020 d'Avocent allie les technologies numérique et analogique afin de permettre un contrôle flexible des serveurs de datacenters et de faciliter le fonctionnement, l'activation et la maintenance des sites distants ne disposant pas d'opérateurs formés. Ce type d'équipement permet à nos clients de bénéficier d'une réduction significative du volume des câbles, d'un accès à distance sécurisé et d'une gestion flexible des serveurs depuis n'importe quel endroit, à n'importe quel moment.

Le dispositif SwitchView IP 1020 est un équipement d'accès à distance KVM (clavier, vidéo et souris) configurable pour une connectivité analogique (locale) ou numérique (distante). Cette configuration est compatible avec des résolutions vidéo de 1280 x 1024 maximum pour l'utilisateur à distance. Les utilisateurs locaux bénéficient d'une qualité vidéo améliorée pouvant aller jusqu'à 1600 x 1200 par l'intermédiaire des voies vidéo.

L'équipement d'accès à distance SwitchView IP 1020, qui fonctionne sur IP, offre un contrôle et une gestion flexibles des équipements cibles depuis n'importe quel endroit dans le monde.

Accès à un équipement d'accès à distance via une connexion réseau

Aucun logiciel ou pilote particulier n'est nécessaire sur les ordinateurs reliés ou clients. Les utilisateurs peuvent accéder à l'équipement d'accès à distance SwitchView IP 1020 et à tous les systèmes reliés via Ethernet à partir d'un ordinateur client, tel qu'un PC. Cet ordinateur client peut être situé n'importe où, tant qu'il est connecté au réseau. Les modes IPv4 (mode par défaut) et IPv6 sont tous deux pris en charge.

Accès simple à tout équipement cible

Lorsque vous sélectionnez un équipement cible, son bureau s'affiche dans le visualiseur vidéo.

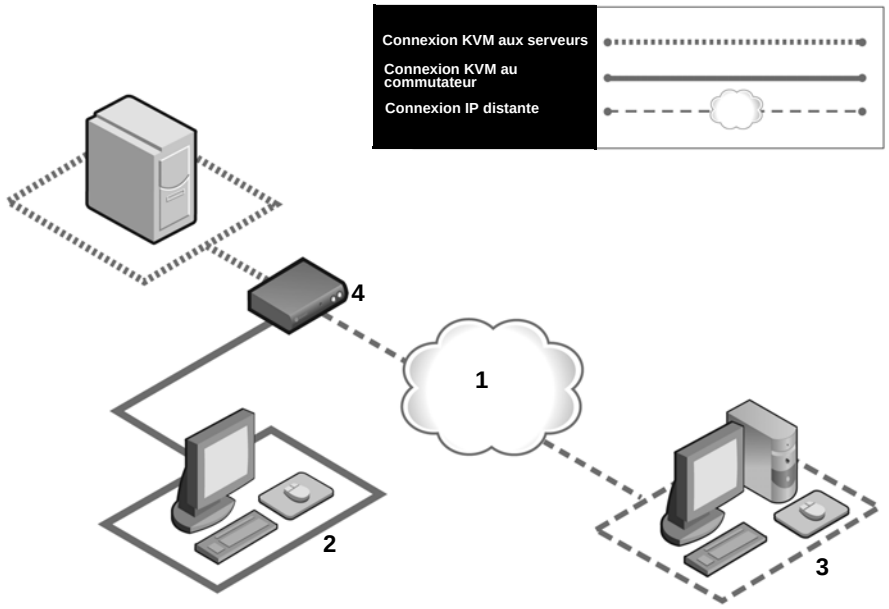

Figure 1.1 : Exemple de configuration d’un équipement d’accès à distance SwitchView IP 1020

Tableau 1.1 : Descriptions de la Figure 1.1

Numéro	Description
1	Ethernet
2	Utilisateur analogique
3	Utilisateur numérique (ordinateur équipé d’un navigateur Internet)
4	Équipement d’accès à distance SwitchView IP 1020

CHAPITRE

2

Installation

Connectivité de l’équipement d’accès à distance SwitchView IP 1020

L’équipement d’accès à distance SwitchView IP 1020 transmet les données du clavier, de la vidéo et de la souris (KVM) entre les opérateurs et les équipements cibles connectés à l'équipement d’accès à distance et reliés au réseau via une connexion Ethernet.

L’équipement d’accès à distance SwitchView IP 1020 utilise le protocole TCP/IP via une connexion Ethernet. Grâce à son interface graphique utilisateur, le serveur Web intégré à l’équipement vous permet d’accéder et de contrôler aisément votre équipement cible.

Installation

Pour configurer et installer un équipement d'accès à distance SwitchView IP 1020, procédez comme suit :

- Déballez le commutateur et assurez-vous que tous les éléments sont présents et en bon état.
- Effectuez tous les branchements entre la source d’alimentation, l’équipement d'accès à distance, les équipements cibles et la connexion Ethernet.
- Mettez l’ensemble sous tension et vérifiez que toutes les connexions fonctionnent.
- Effectuez les réglages nécessaires au niveau des paramètres de la souris.

La Figure 2.1 illustre une configuration de base pour l'équipement d'accès SwitchView IP 1020, en prenant le modèle SwitchView IP 1020 pour exemple. Les descriptions se trouvent dans le Tableau 2.1.

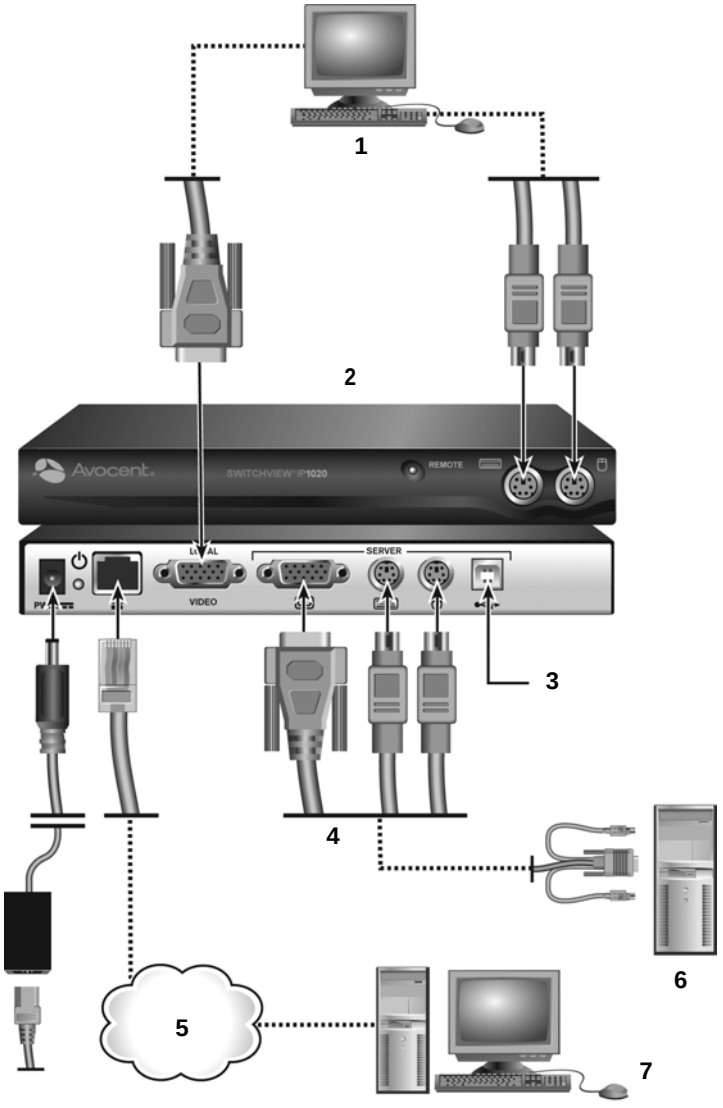

Figure 2.1 : Exemple de configuration de base d’un équipement d’accès à distance SwitchView IP 1020

Tableau 2.1 : Description de la Figure 2.1

Numéro	Description	Numéro	Description
1	Utilisateur local	**5**	Ethernet
2	Équipement d'accès à distance SwitchView IP 1020	6	Serveur
3	Voie USB facultative	**7**	Utilisateur distant
4	Câble CPS2-6A		

Démarrage

Avant d'installer l'équipement d'accès à distance SwitchView IP 1020, consultez les listes ci-dessous pour vous assurer que vous disposez de tous les éléments livrés avec l'équipement d'accès à distance SwitchView IP 1020, ainsi que des autres éléments nécessaires à l'installation.

Éléments fournis avec l'équipement d'accès à distance SwitchView IP 1020

- Adaptateur d'alimentation
- Cordon d'alimentation
- Câble CPS2-6A d'Avocent
- Guide d'installation rapide de l'équipement d'accès à distance SwitchView IP 1020

Autres éléments nécessaires

- Un câble de raccordement CAT 5 pour la connexion du réseau (câble à 4 paires torsadées non blindées)

Configuration de votre réseau

L'équipement d'accès à distance SwitchView IP 1020 utilise des adresses IP pour identifier de manière unique le commutateur et les équipements cibles. La gamme d'équipements d'accès à distance SwitchView IP 1020 prend en charge le protocole DHCP (Dynamic Host Configuration Protocol) ainsi que les adresses IP statiques. Avocent recommande de réserver une adresse IP à chaque équipement d'accès à distance SwitchView IP 1020 et de ne pas modifier ces adresses tant que les commutateurs sont connectés au réseau.

Connexion du matériel de l'équipement d'accès à distance

Raccordement et mise sous tension de l’équipement d’accès à distance SwitchView IP 1020 :

1. Mettez hors tension l’équipement cible à relier au SwitchView IP 1020. Munissez-vous de l’adaptateur et du cordon d’alimentation fournis avec l’équipement d'accès à distance. Raccordez le prolongateur BNC en T au panneau arrière du SwitchView IP 1020, le cordon d’alimentation à l’adaptateur et le connecteur c.a. à une prise de courant alternatif adaptée.

AVERTISSEMENT : La meilleure façon de mettre l’équipement hors tension est de le débrancher.

2. Pour connecter un utilisateur local, raccordez le moniteur VGA à la voie marquée LOCAL VIDEO située sur le panneau arrière de l’équipement d’accès à distance. Branchez les câbles du clavier et de la souris PS/2 dans les voies appropriées à l’avant de l’équipement d’accès à distance.
3. Pour établir une connexion au serveur, raccordez une des extrémités du câble CPS2-6A aux voies souris, clavier et VGA du serveur. Raccordez l’autre extrémité aux voies clavier, souris et VGA situées au niveau de la partie SERVER du panneau arrière du SwitchView IP 1020.

NOTA : En cas d’utilisation de périphériques clavier et souris USB, raccordez un câble USB au serveur. Raccordez ensuite l’autre extrémité de ce câble à la voie USB facultative du SwitchView IP 1020. Le cas échéant, débranchez les connecteurs PS/2 du câble CPS2-6A du serveur.

4. Raccordez un câble de raccordement CAT 5 relié à votre réseau Ethernet à la voie LAN située à l’arrière de l’équipement d’accès à distance SwitchView IP 1020.
5. Mettez sous tension l’équipement cible, puis l’équipement d’accès à distance SwitchView IP 1020. Au bout d’une minute environ, l’équipement termine l’initialisation et affiche les données vidéo de l’équipement cible sur le moniteur connecté à la voie locale.
6. Dans le navigateur web, saisissez l’adresse IP par défaut (https://192.168.1.254) pour accéder à l’équipement.
7. Connectez-vous à l’explorateur du SVIP1020 puis, dans la barre de menu supérieure, sélectionnez *Appliance (Matériels)-Appliance Settings (Paramètres du matériel)-Network (Réseau)*. Saisissez les informations relatives à l’adresse de votre réseau.

NOTA : Par défaut, le nom d’utilisateur est Admin et il n’y a pas de mot de passe.

Voyants du SwitchView IP 1020

Le panneau avant de l'équipement d'accès à distance SwitchView IP 1020 est doté d'un voyant bleu indiquant qu'une connexion à distance est en cours. Le voyant vert situé sur le panneau arrière indique que l'équipement est sous-tension. Si ce voyant clignote de façon continue, cela signifie que l'équipement est en mode de récupération.

Le panneau arrière comporte également deux voyants relatifs à la connexion LAN :

- Un voyant vert s'allume lorsque la connexion au réseau est correctement établie ; il clignote lorsque la voie est active.

Un voyant orange s'allume lorsque la communication s'effectue à 100 Mbit/s via une connexion Ethernet.

Réglage des paramètres de la souris sur les équipements cibles

Avant de pouvoir utiliser un ordinateur relié à l'équipement d'accès à distance SwitchView IP 1020 pour une utilisation à distance, un réglage de la vitesse de la souris doit être effectué et l'accélération doit être désactivée. Il est conseillé d'utiliser le pilote de souris PS/2 par défaut pour les machines fonctionnant sous Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003).

Pour s'assurer que le mouvement de la souris locale et l'affichage du curseur distant soient synchronisés, l'accélération de la souris doit être réglée sur « aucun » pour tous les comptes utilisateurs ayant accès à l'ordinateur cible à l'aide de l'équipement d'accès à distance SwitchView IP 1020. L'accélération de la souris doit également être réglée sur « aucun » sur tous les systèmes distants. N'utilisez pas de curseur spécial. Les options de visibilité du curseur (telles que les traînées du pointeur, les animations d'emplacement du curseur à l'aide de la touche **Ctrl**, l'ombre du curseur et le curseur masqué) doivent être également désactivées.

CHAPITRE

3

Utilisation de l’interface Web

Interface Web intégrée

L’équipement d’accès à distance SwitchView IP 1020 est équipé d’une interface Web intégrée permettant de gérer l’accès à distance. L’interface Web intégrée de l'équipement d'accès à distance offre, par l’intermédiaire d’un navigateur Web, un accès sécurisé à tout équipement relié à l'équipement d'accès à distance SwitchView IP 1020 d’un simple clic.

Le Tableau 3.1 recense les systèmes d’exploitation et navigateurs pris en charge par l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020.

Tableau 3.1 : Systèmes d’exploitation et navigateurs pris en charge par l’interface Web intégrée

	Navigateur		
Système d’exploitation	**Microsoft® Internet Explorer 6.0 SP1 et versions ultérieures**	**Mozilla versions 1.7.3 et ultérieures**	**Firefox versions 1.0 et ultérieures**
Windows 2000 Workstation ou Server avec Service Pack 2	Oui	Oui	Oui
Windows Server 2003 Standard, Enterprise ou Web Edition	Oui	Oui	Oui
Windows XP Édition Familiale, ou Professionnel	Oui	Oui	Oui
Red Hat Enterprise Linux 3 et 4	Non	Oui	Oui
Sun Solaris 9 et 10	Non	Oui	Oui
Novell SUSE® Linux Enterprise 9 et 10	Non	Oui	Oui
Fedora Core 4 et 5	Non	Oui	Oui
Mac OS X Tiger (10.4+)	Non	Non	Oui

NOTA : Firefox 1.5 (ou version ultérieure) requis pour Mac OS X.

Avocent recommande d’utiliser la dernière version disponible du navigateur.

Un visualiseur vidéo permet de contrôler en temps réel les fonctions du clavier, du moniteur et de la souris de chaque équipement cible relié à l’équipement d’accès à distance SwitchView IP 1020. Vous avez également la possibilité d’utiliser des macros prédéfinies pour réaliser des actions dans la fenêtre du visualiseur. Les instructions d’utilisation du visualiseur vidéo sont décrites au Chapitre 4. Une fois que vous avez installé et configuré le commutateur tel que décrit dans le Chapitre 2, et que vous avez défini l’adresse IP, vous êtes prêt à démarrer.

Connexion à l’équipement d’accès à distance SwitchView IP 1020

NOTA : L’équipement d’accès à distance SwitchView IP 1020 démarre avec l’adresse IP statique, la passerelle et le masque de sous-réseau suivants :
Adresse IP : 192.168.1.254
Passerelle : 192.168.1.1
Masque de sous-réseau : 255.255.255.0

Pour lancer une session KVM, vous devez d'abord vous connecter à l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020.

Connexion à l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 :

1. Lancez un navigateur web.
2. Saisissez l’adresse IP ou le nom d’hôte attribué à l'équipement d'accès à distance SwitchView IP 1020 auquel vous souhaitez accéder dans la barre d'adresse du navigateur. Utilisez le format https://xxx.xx.xx.xx ou https://nomdhote.
3. Lorsque la communication entre le navigateur et le commutateur est établie, saisissez votre nom d’utilisateur et votre mot de passe puis cliquez sur *Login* (Connexion). L'explorateur du SwitchView IP 1020 s'affiche.

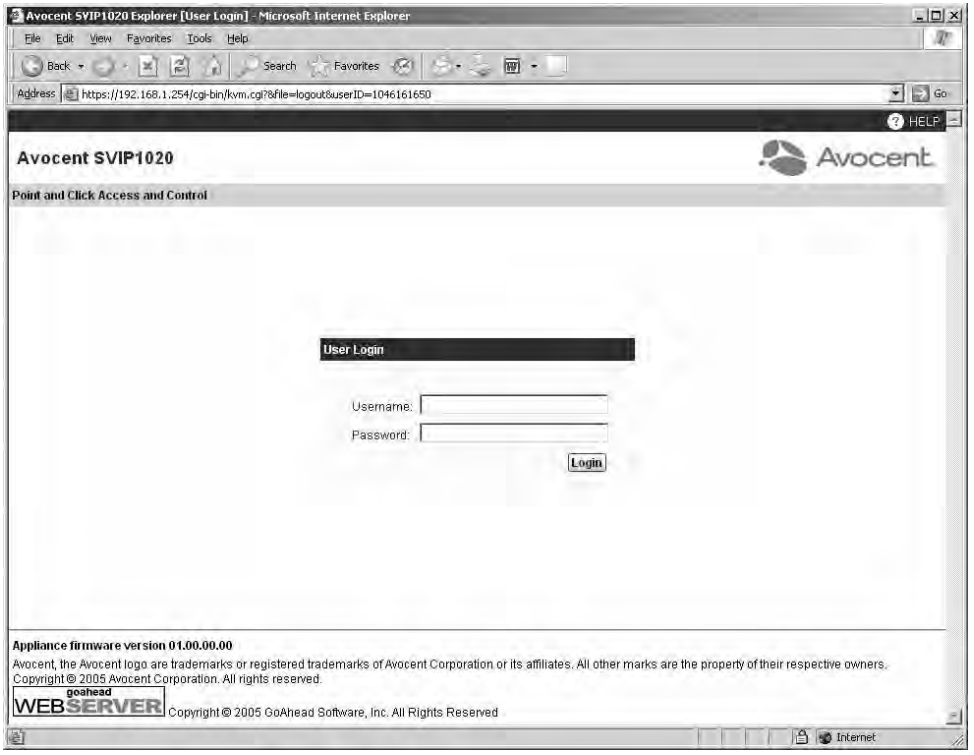
Avocent SVIP1020 Explorer [User Login] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.254/cgi-bin/kvm.cgi?&file=logout&userID=1046161650
HELP
Avocent SVIP1020
Avocent
Point and Click Access and Control
User Login
Username:
Password:
Login
Appliance firmware version 01.00.00.00
Avocent, the Avocent logo are trademarks or registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.
Copyright © 2005 Avocent Corporation. All rights reserved.
goahead
WEBSERVER
Copyright © 2005 GoAhead Software, Inc. All Rights Reserved
Internet

Figure 3.1 : Écran User Login (Connexion de l'utilisateur) de l'explorateur du SVIP 1020

NOTA : Par défaut, le nom d’utilisateur est Admin et il n’y a pas de mot de passe.

Fenêtre SwitchView IP 1020 Explorer (Explorateur du SwitchView IP 1020)

La fenêtre de l'explorateur du SwitchView IP 1020 d'Avocent s’affiche après connexion et authentification d’un utilisateur. Cette fenêtre vous permet de visualiser, d'accéder et de gérer l’équipement d’accès à distance SwitchView IP 1020. Elle permet également de définir les paramètres système et de modifier les paramètres de profil.

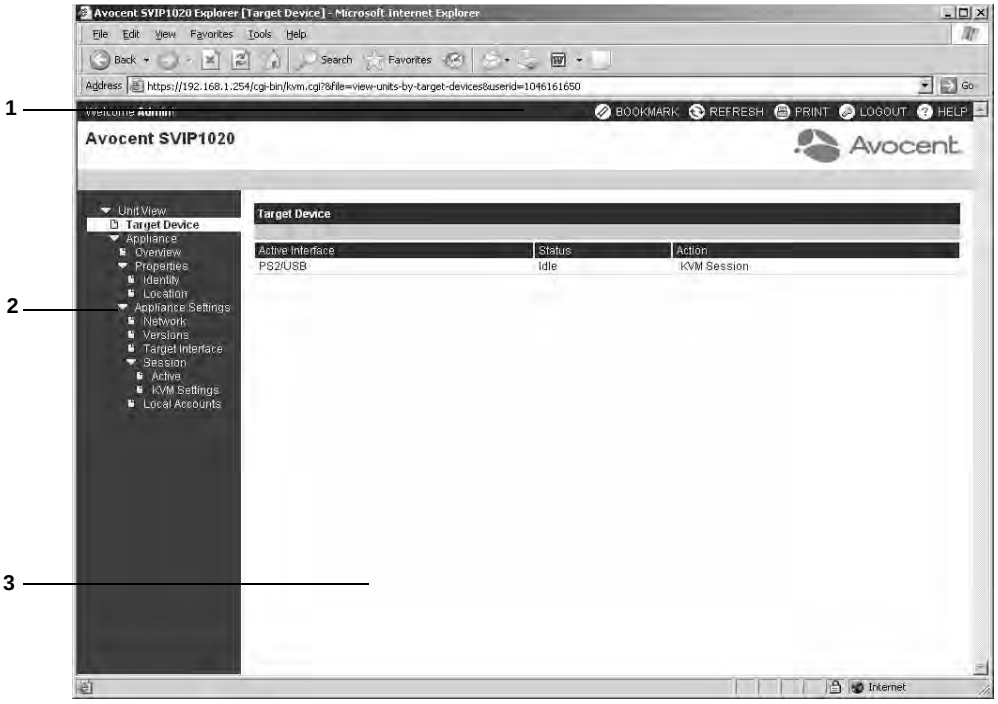

Figure 3.2 : Fenêtre de l'explorateur du SwitchView IP 1020 d'Avocent

Tableau 3.2 : Description de la Figure 3.2

Numéro	Description
1	Barre d’options supérieure : permet de mettre en signet une fenêtre de l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020, d'actualiser l’affichage de cette fenêtre, d'imprimer une page Web, de quitter une session logicielle ou d'accéder à la page d’aide de l’assistance technique d’Avocent. Le nom de l’utilisateur connecté apparaît dans la partie gauche de la barre d’options supérieure.
2	Barre de navigation latérale : permet d'afficher dans la zone de contenu les informations relatives au système de votre choix pour les visualiser ou les modifier. Cette barre contient également des icônes, dans le coin supérieur gauche, permettant de développer ou de réduire l’arborescence.
3	Zone de contenu : permet d'afficher les informations ou modifications relatives à l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020.

Utilisation de la barre de navigation latérale

Vous pouvez utiliser la barre de navigation latérale pour afficher des fenêtres dans lesquelles vous spécifierez des paramètres ou effectuerez des opérations. Cliquez sur un lien non précédé d’une flèche pour afficher la fenêtre correspondante.

Utilisation de la barre d’options supérieure

Mise en signet d’une fenêtre

La barre d’options supérieure de la fenêtre de l'explorateur du SwitchView IP 1020 comporte une icône de mise en signet. La mise en signet d’une fenêtre ajoute un lien vers cette fenêtre dans le menu Favoris. Sélectionnez ce lien à tout moment pour accéder rapidement à la fenêtre.

Si vous mettez en signet une fenêtre et que les informations qu’elle contient sont modifiées, les informations mises à jour apparaissent lors du prochain affichage de la fenêtre.

Si vous cliquez sur *BOOKMARK* (Mise en signet) ou sur l’icône correspondante après expiration de la session de l’interface Web de l'équipement d'accès à distance SwitchView IP 1020, la fenêtre de connexion de utilisateur s’affiche, vous invitant à ouvrir une nouvelle session.

Mise en signet d’une fenêtre :

1. Dans la barre d’options supérieure, cliquez sur *BOOKMARK* ou sur l’icône correspondante. La boîte de dialogue Add Favorite (Ajouter aux favoris) s’affiche.
2. Si vous le souhaitez, nommez la fenêtre. Vous pouvez également cliquer sur le bouton *Create in* (Créer dans) pour créer ou indiquer un dossier dans lequel placer le lien.
3. Cliquez sur *OK* pour fermer la boîte de dialogue Add Favorite (Ajouter aux favoris).

Impression d’une fenêtre

La barre d'options supérieure de toutes les fenêtres de l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 comporte une icône d’impression.

Impression d'une fenêtre de l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 :

1. Dans la barre d’options supérieure, cliquez sur *PRINT* (IMPRIMER) ou sur l’icône correspondante. La boîte de dialogue d'impression s’affiche.
2. Définissez les options d’impression de votre choix.
3. Cliquez sur *Print* pour imprimer le contenu de la fenêtre et fermer la boîte de dialogue d'impression.

Actualisation d’une fenêtre

Pour actualiser le contenu d’une fenêtre de l’explorateur du SwitchView IP 1020 à tout moment, cliquez sur *REFRESH* (ACTUALISER) ou sur l’icône correspondante dans la barre d’options supérieure.

Déconnexion

Pour vous déconnecter à tout moment, cliquez sur l’icône de déconnexion dans la barre d’options supérieure.

Gestion des comptes locaux

L’interface Web de l'équipement d'accès à distance offre des fonctions de sécurité locale et de connexion par l’intermédiaire de comptes utilisateurs définis par l’administrateur. La fonction *Local Accounts* (Comptes locaux) de la barre de menus latérale permet aux administrateurs d’ajouter ou de supprimer des utilisateurs, de définir les niveaux de préemption et d’accès et de modifier les mots de passe.

Niveaux d’accès utilisateur

Les comptes présentent deux niveaux d’accès : utilisateur et administrateur. La plupart des tâches de gestion du commutateur sont accessibles uniquement aux administrateurs.

Niveaux de préemption

Le niveau de préemption des utilisateurs détermine leur capacité ou non à déconnecter la session série ou vidéo (KVM) d’un autre utilisateur sur un équipement cible.

Les administrateurs de l’interface Web de l'équipement d'accès à distance définissent le niveau de préemption des utilisateurs lors de la création des comptes. Il est possible de modifier ce niveau ultérieurement.

Les niveaux de préemption vont de 1 à 4, 4 étant le niveau le plus élevé. Par exemple, un utilisateur bénéficiant d’un niveau de préemption 4 peut préempter la session d’autres utilisateurs de niveau 4 ainsi que ceux ayant un niveau de 1, 2 ou 3.

Ajout d’un nouveau compte utilisateur (pour l’administrateur uniquement) :

1. Dans la barre de menus latérale, sélectionnez *Local Accounts*. La liste des utilisateurs s’affiche.
2. Cliquez sur le bouton *Add* (Ajouter).
3. Saisissez le nom et le mot de passe du nouvel utilisateur dans les espaces prévus à cet effet.
4. Sélectionnez les niveaux de préemption et d’accès.
5. Cliquez sur le bouton *Save* (Enregistrer) pour terminer le processus.

Suppression d’un compte utilisateur (pour l’administrateur uniquement) :

1. Dans la barre de menus latérale, sélectionnez *Local Accounts*. La liste des utilisateurs s’affiche.
2. Activez la case en regard de chacun des comptes à supprimer puis cliquez sur le bouton Delete (Supprimer).

Modification d’un compte utilisateur (pour l’administrateur ou l’utilisateur actif uniquement) :

1. Dans la barre de menus latérale, sélectionnez Local accounts. La liste des utilisateurs s’affiche.
2. Cliquez sur le nom de l’utilisateur dont le compte est à modifier. Un profil d’utilisateur s’affiche.
3. Modifier le compte utilisateur, puis cliquez sur *Save*.

Gestion des propriétés des équipements

Affichage et modification des paramètres de configuration du matériel

L’équipement d’accès à distance SwitchView IP 1020 peut afficher la plupart des propriétés des équipements reliés dans la fenêtre du navigateur Web de l'équipement d'accès à distance.

NOTA : Les utilisateurs peuvent visualiser toutes les informations concernant le matériel mais seul l’administrateur peut modifier les paramètres.

Tableau 3.3 : Affichage des informations relatives au matériel

Objectif	Sélection
Afficher le nom ou le type de l’unité	*Appliance - Overview (Matériel - Vue d’ensemble)*
Afficher la liste des équipements cibles disponibles, leur type et leur état	*Target Device (Équipement cible)*
Saisir, modifier ou afficher la version IP de l'unité, l’adresse de réseau, l’adresse de passerelle, le masque de sous-réseau, l’adresse MAC, la vitesse de transmission du réseau local, l’état d’activation DHCP ou l’état de réponse à l’utilitaire ping ICMP	*Appliance - Appliance Settings - Network (Matériel - Paramètres du matériel - Réseau)* **NOTA :** Si l'option DHCP est activée avant de modifier le mode IP sur IPv4 ou IPv6, l'utilisateur doit vérifier que le serveur DHCP comporte une adresse IP prédéfinie, associée à l'adresse MAC de l'équipement d'accès à distance.
Afficher la version du firmware de l’unité pour l’application, le redémarrage et le FPGA de la vidéo	*Appliance - Appliance Settings - Versions (Matériel - Paramètres du matériel - Versions)*
Afficher la liste des sessions KVM actives et leur durée	*Appliance - Appliance Settings - Sessions - Active (Matériel - Paramètres du matériel - Sessions - Active)*
Afficher le numéro de référence, le numéro de série et le numéro EID de l’unité	*Appliance - Properties - Identity (Matériel - Propriétés - Identité)*
Saisir ou afficher le site, le service et l’emplacement de l’unité	*Appliance - Properties - Location (Matériel - Propriétés - Emplacement)*
Activer le délai d’expiration dû à l’inactivité	*Appliance - Appliance Settings - Sessions - KVM settings (Matériel - Paramètres du matériel - Sessions - Paramètres KVM)* Cochez ensuite la case *Enable Inactivity timeout* (Activer délai d’expiration).
Modifier le niveau de cryptage de l’unité	*Appliance - Appliance Settings - Sessions - KVM settings (Matériel - Paramètres du matériel - Sessions - Paramètres KVM)* Sélectionnez ensuite le niveau de cryptage de votre choix pour les signaux du clavier et de la souris puis pour les signaux vidéo.

Configuration LDAP

LDAP est un protocole standard utilisé pour accéder à un annuaire, lui transmettre des requêtes et le mettre à jour à l'aide du protocole TCP/IP. Conçu sur le modèle des services d'annuaire X.500, LDAP présente une structure d'annuaire général bénéficiant de fonctionnalités de sécurité renforcée pour l'authentification, la confidentialité et l'intégrité.

Si des comptes utilisateurs individuels sont stockés sur un service d'annuaire activé par le protocole LDAP, par exemple Active Directory, celui-ci peut être utilisé pour l'authentification des utilisateurs. Les valeurs par défaut attribuées aux paramètres de recherche et de requête LDAP sont définies pour une utilisation avec Active Directory.

Vous pouvez configurer vos paramètres d'authentification via les paramètres de l'interface Web intégrée. Le logiciel envoie le nom d'utilisateur, le mot de passe et d'autres informations au matériel, qui détermine alors si l'utilisateur est autorisé ou non à afficher ou modifier les paramètres de configuration via l'interface Web intégrée.

NOTA : Sauf indication contraire, les valeurs LDAP par défaut doivent être utilisées, à moins qu'Active Directory n'ait été reconfiguré. La modification des valeurs par défaut risque d'entraîner des erreurs de communication avec le serveur d'authentification LDAP.

Paramètres de la page Vue d'ensemble LDAP

Dans la page LDAP Overview (Vue d'ensemble LDAP) de l'interface Web intégrée, vous pouvez configurer la priorité de l'authentification LDAP, ainsi que les informations de connexion au serveur LDAP.

Priorité de l'authentification LDAP

Dans la section LDAP Priority (Priorité LDAP) de la page LDAP Overview, vous pouvez désactiver l'authentification LDAP ou bien définir la priorité de l'authentification en choisissant laquelle de l'authentification locale ou LDAP doit être effectuée en premier.

Configuration des paramètres de priorité de l'authentification LDAP :

1. Sélectionnez *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview* (Matériel - Paramètres du matériel - Comptes utilisateurs - Comptes LDAP - Vue d'ensemble).
2. Dans la section LDAP Priority, sélectionnez *LDAP Disabled* (Authentification LDAP désactivée), *LDAP before Local* (Authentification LDAP avant locale) ou *LDAP after Local* (Authentification LDAP après locale).
3. Cliquez sur *Save*.

Serveurs LDAP

Les champs Address (Adresse) indiquent les noms d'hôte ou les adresses IP des serveurs LDAP principal et secondaire. Le deuxième serveur LDAP est facultatif.

Les champs Port (Voie) indiquent les numéros des voies UDP (User Datagram Protocol) utilisées pour communiquer avec les serveurs LDAP. La valeur par défaut est 389 pour le protocole LDAP non sécurisé et 636 pour le protocole LDAP sécurisé (LDAPS). Le champ ID de la voie est renseigné automatiquement par le logiciel lorsqu'un type d'accès est spécifié.

Les boutons radio Access Type (Type d'accès) permettent de sélectionner le mode de transmission des requêtes à chaque équipement cible LDAP. Si vous sélectionnez LDAP, tous les noms d'utilisateurs, les mots de passe, etc., échangés entre le matériel et le serveur LDAP sont envoyés sous forme de texte en clair, non sécurisé. Sélectionnez LDAPS pour une communication sécurisée, cryptée, entre le matériel et le serveur LDAP.

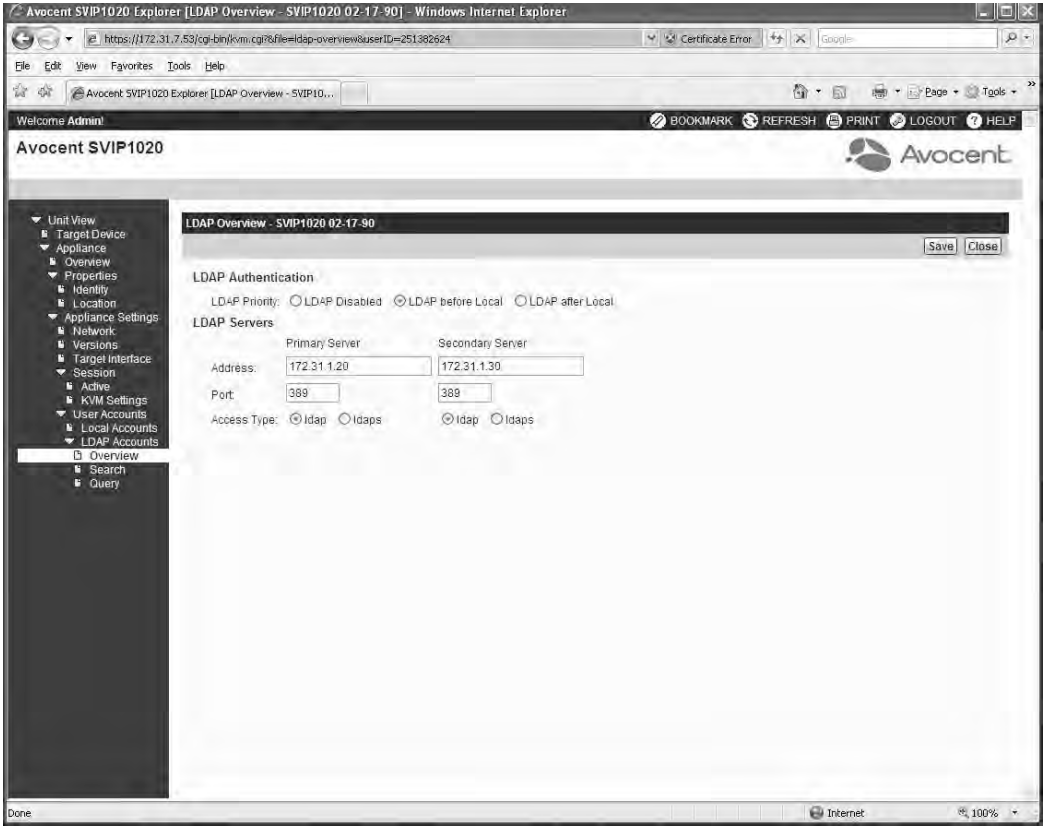

Figure 3.3 : Page LDAP Overview de l'interface Web intégrée

Configuration des paramètres du serveur LDAP :

1. Sélectionnez *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview* (Matériel - Paramètres du matériel - Comptes utilisateurs - Comptes LDAP - Vue d'ensemble).
2. Indiquez l'adresse des serveurs primaire et secondaire, ainsi que la voie et le type d'accès dans les champs ou à l'aide des boutons radio prévus à cet effet.
3. Cliquez sur *Save*.

Paramètres de la page LDAP Search (Recherche LDAP)

Dans la page LDAP Search, vous pouvez configurer les paramètres de recherche des utilisateurs du service d'annuaire LDAP.

Le champ Search DN (Recherche par DN) permet de définir un utilisateur de type administrateur dont les références de connexion sont utilisées pour la connexion au service d’annuaire. Une fois le matériel authentifié, le service d’annuaire lui donne accès à l’annuaire afin qu’il transmette les requêtes d’authentification de l’utilisateur spécifiées à la page Query (Requête). Les valeurs par défaut sont : cn=Administrator, cn=Users, dc=yourDomainName et dc=com. Elles sont modifiables. Par exemple, pour définir le DN (Distinguished Name) d'un administrateur pour test.view.com, saisissez **cn=Administrator, cn=Users, dc=test, dc=view** et **dc=com.** Ce champ est obligatoire, à moins que le service d’annuaire n’ait été configuré de sorte à permettre les recherches anonymes, ce qui ne fait pas partie de la configuration par défaut. Les valeurs du champ Search DN doivent être séparées par des virgules.

Le champ Search Password (Mot de passe de recherche) sert à identifier l'administrateur ou l'utilisateur spécifié dans le champ Search DN.

Le champ Search Base (Base de recherche) sert à définir le point de départ de la recherche LDAP. Les valeurs par défaut sont dc=yourDomainName et dc=com. Elles sont modifiables. Par exemple, pour définir le point de départ de la recherche sur test.com, saisissez **dc=test, dc=com**. Les valeurs du champ Search Base doivent être séparées par des virgules.

Le champ UID Mask (Masque UID) sert à définir les critères de recherche des identifiants utilisateur sur les équipements cibles LDAP. Le format suivant doit être utilisé : <name>=<%1>. La valeur par défaut est sAMAccountName=%1 et est compatible avec Active Directory. Cette information est obligatoire lors des recherches LDAP.

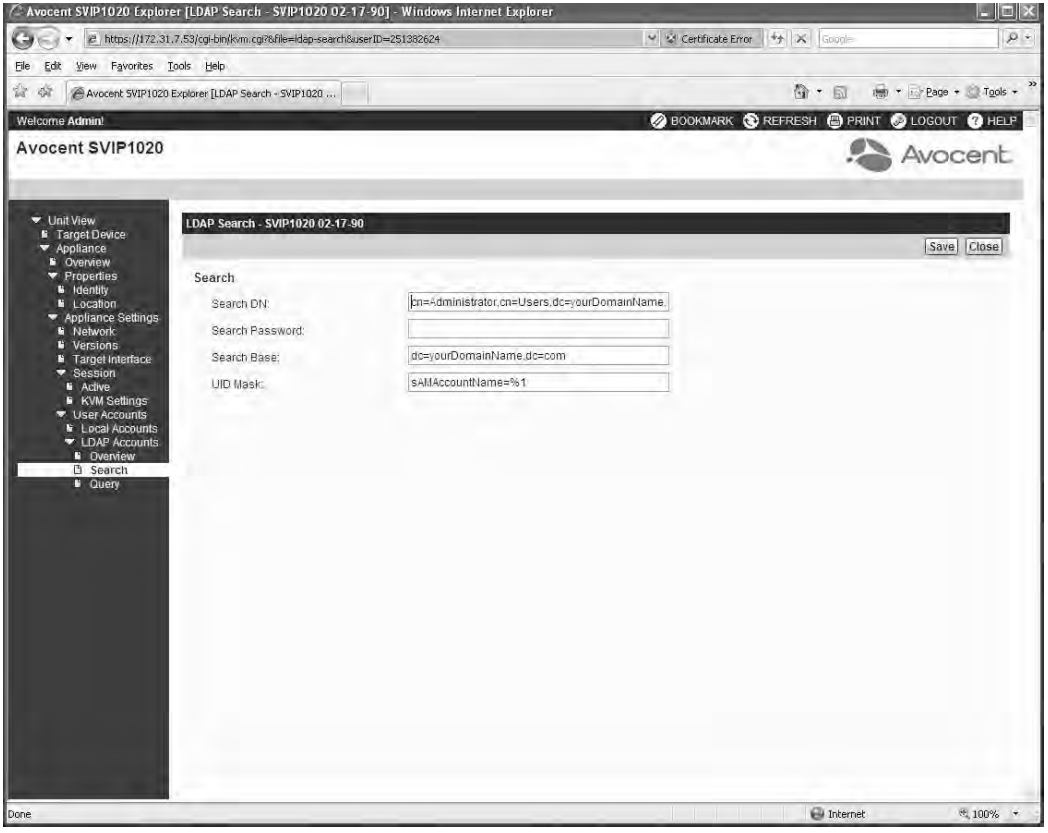

Figure 3.4 : Page LDAP Search de l'interface Web intégrée

Configuration des paramètres de recherche LDAP :

1. Sélectionnez *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Search* (Matériel - Paramètres du matériel - Comptes utilisateurs - Comptes LDAP - Recherche).
2. Entrez les informations dans les champs Search DN, Search Password, Search Base et UID Mask.
3. Cliquez sur *Save*.

NOTA : Vous ne pouvez pas modifier ces options si la case *LDAP Disabled* est cochée dans la section LDAP Priority de la page Overview.

Paramètres de la page LDAP Query (Requête LDAP)

Dans la page LDAP Query, vous pouvez configurer les paramètres utilisés pour lancer des requêtes d'authentification de l'utilisateur.

Le matériel émet deux types de requêtes. Le mode de requête matériel sert à identifier les administrateurs essayant de se connecter directement au matériel. Le mode de requête équipement cible sert à identifier les utilisateurs essayant de se connecter aux équipements cibles reliés. De plus, chaque type de requête peut être transmis selon trois modes basés sur certaines informations permettant de déterminer si un utilisateur est autorisé ou non à accéder au matériel ou aux équipements cibles reliés. Reportez-vous à la section *Modes de requête matériel et équipement cible* à la page 22 pour de plus amples informations sur ces modes.

Vous pouvez configurer les paramètres suivants sur la page LDAP Query :

- Les paramètres Query Mode (Appliance) (Mode de requête matériel) déterminent si l'utilisateur dispose ou non d’un accès au matériel.
- Les paramètres du Query Mode (Target Device) (Mode de requête équipement cible) déterminent si l'utilisateur dispose ou non de droits d’accès de type utilisateur pour se connecter aux équipements reliés au matériel. L’utilisateur n’a pas accès aux paramètres du matériel.
- Les champs Group Container (Conteneur de groupe), Group Container Mask (Masque de conteneur de groupe) et Target Mask (Masque cible) sont utilisés uniquement avec les modes de requête de type Groupe. Ces informations sont obligatoires lors d'une requête portant sur un matériel ou un équipement.
- Le champ Group Container indique l’unité organisationnelle créée dans Active Directory par l’administrateur définissant l’emplacement des objets du groupe. Les objets du groupe sont des objets Active Directory pouvant contenir des utilisateurs, des ordinateurs, des contacts et d’autres groupes. Le conteneur de groupe est utilisé avec le mode de requête Group Attribute (Attribut de groupe). Chaque objet du groupe est affecté à des membres (personne, matériel et équipements cibles) disposant d'un certain niveau d'accès. Le niveau d’accès associé à un groupe est configuré en définissant la valeur d’un attribut de l’objet du groupe. Par exemple, si la propriété Notes de l’objet du groupe sert à définir l’attribut de contrôle d’accès, le champ Access Control Attribute (Attribut de contrôle d’accès) de la page LDAP Query doit avoir la valeur info. Si la propriété Notes est définie avec la valeur KVM User Admin (Administrateur d’utilisateur KVM), les membres de ce groupe disposent de droits d’accès de type administrateur d’utilisateur pour se connecter aux matériels et aux équipements cibles membres du même groupe.
- La propriété Notes permet de définir l’attribut de contrôle d’accès. La valeur de la propriété Notes, disponible dans les objets de groupe et d’utilisateur indiqués au niveau d’Active Directory Users and Computers (ADUC), est enregistrée en interne dans l’annuaire, sous la valeur d’un attribut info. ADUC est un composant logiciel enfichable de Microsoft Management Console utilisé pour la configuration d’Active Directory. Pour le lancer, sélectionnez *Démarrer - Programmes - Outils d'administration - Utilisateurs et Ordinateurs d’Active Directory.* Cet outil permet de créer, configurer et supprimer des objets tels que les utilisateurs, les ordinateurs et les groupes.

- Le champ Group Container Mask permet de définir le type d'objet du conteneur de groupe, généralement une unité organisationnelle. La valeur par défaut est « ou=%1 ».
- Le champ Target Mask permet de définir un filtre de recherche pour l’équipement cible. La valeur par défaut est « cn=%1 ».
- Le champ Access Control Attribute permet d'indiquer le nom de l’attribut utilisé avec les modes de requête Attribute. La valeur par défaut est info.

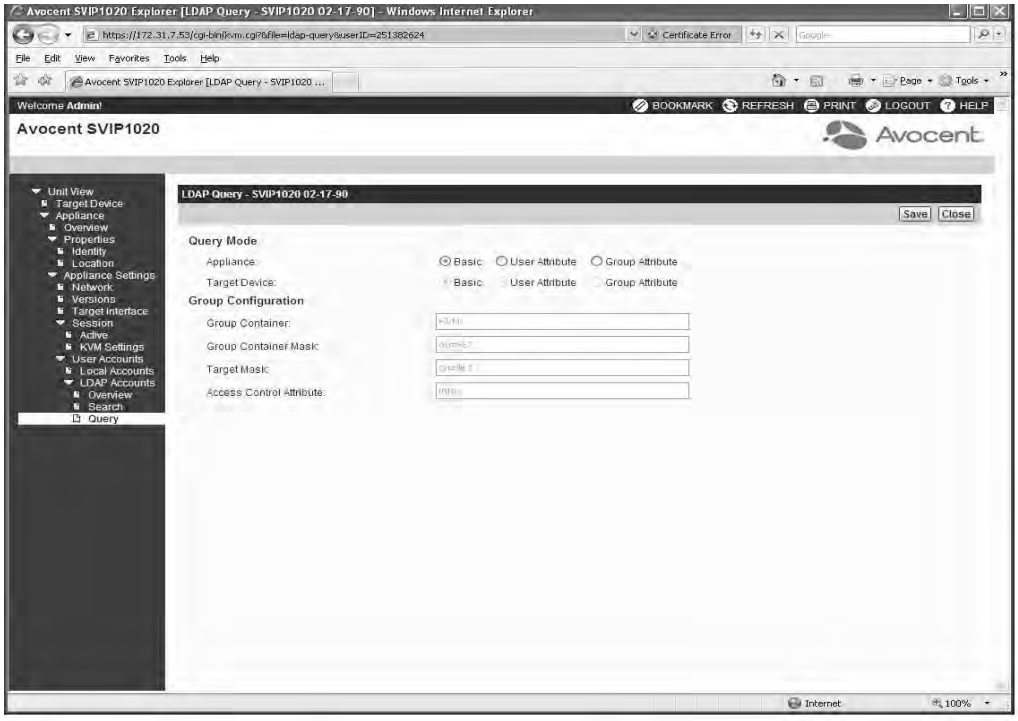

Figure 3.5 : Page LDAP Query de l'interface Web intégrée

Configuration des paramètres de requête LDAP :

1. Sélectionnez *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Query* (Matériel - Paramètres du matériel - Comptes utilisateurs - Comptes LDAP - Requête).
2. Sélectionnez *Basic* (Simple), *User Attribute* (Attribut d'utilisateur) ou *Group Attribute* pour le mode de requête matériel (Appliance Query Mode) et le mode de requête équipement cible (Target Device Query Mode).
3. Renseignez les champs Group Container, Group Container Mask, Target Mask et Access Control Attribute.
4. Cliquez sur *Save*.

NOTA : Vous ne pouvez pas modifier ces options si la case *LDAP Disabled* est cochée dans la section LDAP Priority de la page Overview.

Modes de requête matériel et équipement cible

Trois modes différents peuvent être utilisés pour le mode de requête matériel et le mode de requête équipement cible :

- Basic : une requête portant sur le nom d’utilisateur et le mot de passe de l’utilisateur est transmise au service d’annuaire. Si les données sont vérifiées, l’utilisateur dispose alors de droits d’accès de type administrateur pour le matériel et les équipements cibles qui lui sont reliés en mode de requête matériel ou à n'importe quel équipement sélectionné en mode de requête équipement cible.
- User Attribute : une requête portant sur le nom d’utilisateur, le mot de passe et un attribut de contrôle d’accès pour l’utilisateur du matériel est transmise au service d’annuaire. L’attribut de contrôle d’accès est lu à partir de l’objet utilisateur (le compte utilisateur) d’Active Directory.

  Si la valeur KVM Appliance Admin (Administrateur de matériel KVM) est trouvée, l’utilisateur dispose de droits d’accès de type administrateur de matériel pour le matériel et les équipements cibles qui lui sont reliés en mode de requête matériel ou à tout équipement cible sélectionné pour le mode de requête équipement cible. Si la valeur KVM User Admin est trouvée, l’utilisateur dispose de droits d’accès de type administrateur d'utilisateur pour le matériel et les équipements cibles qui lui sont reliés en mode de requête matériel ou à tout équipement cible sélectionné pour le mode de requête équipement cible.

  Les exemples suivants vous montrent comment sont définis les modes d’attribut KVM Appliance Admin et KVM User Admin dans Active Directory pour un utilisateur du nom de John Smith, enregistré dans le composant ADUC. Pour accéder à ce dernier, sélectionnez *Démarrer - Programmes - Outils d’administration - Utilisateurs et Ordinateurs d’Active Directory*.

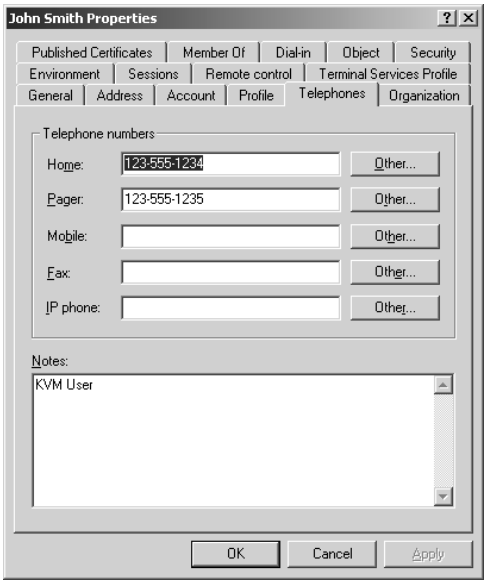

Figure 3.6 : Utilisateur KVM dans Active Directory

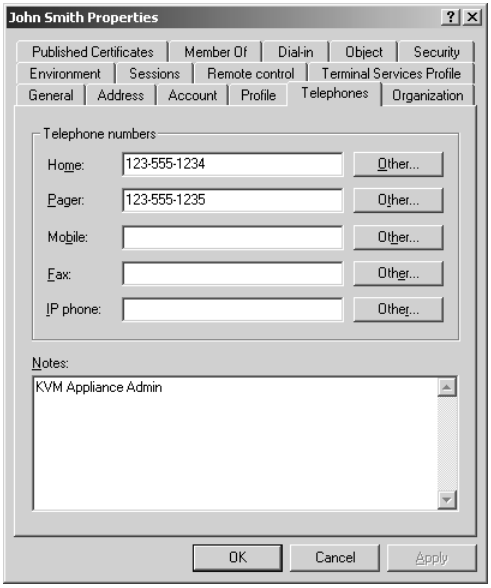

Figure 3.7 : Administrateur de matériel KVM dans Active Directory

- Group Attribute : une requête portant sur le nom d'utilisateur, le mot de passe et le groupe est transmise au service d'annuaire pour un matériel et ses équipements cibles reliés en mode de requête matériel ou pour un équipement cible sélectionné en mode de requête équipement cible. Si un groupe contenant le nom d'utilisateur et le nom du matériel est trouvé, l'utilisateur dispose de droits d'accès au matériel ou aux équipements cibles qui lui sont reliés, selon le contenu du groupe lorsque le mode de requête matériel est utilisé. Si un groupe contenant l'ID utilisateur et l'ID de l'équipement cible est trouvé, l'utilisateur dispose de droits d'accès aux équipements spécifiés reliés au matériel lorsque le mode de requête équipement cible est utilisé.

  La structure des groupes peut comporter jusqu'à 16 niveaux. Vous pouvez créer des groupes au sein des groupes existants. Par exemple, vous pouvez avoir un groupe de premier niveau appelé Computers (Ordinateurs), contenant un élément R&D représentant également un groupe. Le groupe R&D peut contenir à son tour un élément appelé Domestic (Domestique), lequel est également un groupe, etc.

  L'exemple suivant montre des groupes définis dans Active Directory.

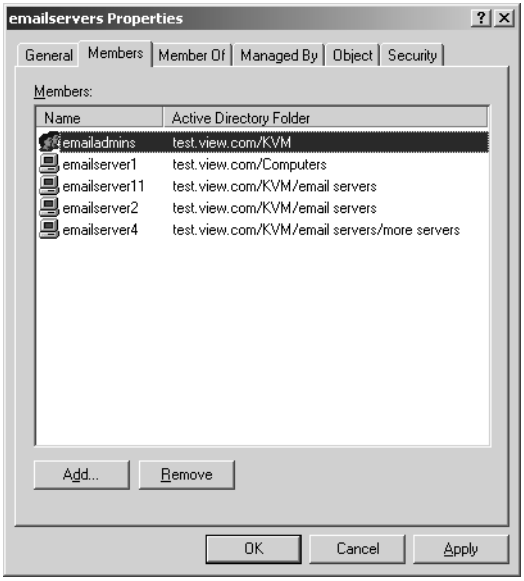

Figure 3.8 : Groupes définis dans Active Directory

Configuration d'Active Directory pour la transmission de requêtes

Avant de pouvoir utiliser l'un des modes de requête pour les unités, vous devez modifier les paramètres d'Active Directory afin que le mode de requête sélectionné puisse attribuer les droits d'accès correspondant à l'utilisateur.

Définition de requêtes de groupe :

1. Connectez-vous sous Windows en tant qu’administrateur.
2. Ouvrez le logiciel Active Directory.
3. Créez une unité organisationnelle représentant un conteneur de groupe.
4. Créez un objet dans Active Directory portant un nom identique à celui du système de commutation en mode de requête matériel (indiqué dans la fenêtre de vue d'ensemble du matériel de l'interface Web intégrée) ou identique aux équipements cibles qui lui sont reliés en mode de requête équipement. Les noms doivent être exactement identiques et respecter la même casse.
5. Les noms des matériels et des équipements cibles utilisés pour les requêtes de groupe sont enregistrés dans le matériel. Le nom du matériel indiqué dans la fenêtre de vue d'ensemble du matériel de l'interface Web intégrée et ceux des équipements cibles doivent correspondre exactement aux noms d'objets dans Active Directory. Chaque nom peut être constitué de toute combinaison de caractères alphabétiques en majuscule ou minuscule (a à z, A à Z), de chiffres (0 à 9) et de traits d’union (-). Les espaces et les points (.) ne sont pas autorisés et un nom ne peut pas comporter uniquement des chiffres. Ces contraintes sont liées à Active Directory.

NOTA : Dans les premières versions, le nom par défaut du matériel défini en usine comporte un espace qu'il est nécessaire de supprimer dans la fenêtre de vue d'ensemble du matériel de l'interface Web intégrée.

6. Créez un ou plusieurs groupe(s) dans l’unité organisationnelle du conteneur de groupe.
7. Ajoutez les noms d’utilisateurs et les objets matériel et équipement cible aux groupes que vous avez créés à l’étape 5.

Spécifiez la valeur de tout attribut utilisé pour implémenter l’attribut de contrôle d’accès. Par exemple, si vous utilisez info comme attribut dans le champ Access Control Attribute et la propriété Notes de l'objet de groupe pour implémenter l'attribut de contrôle d'accès, la valeur de l'attribut Notes dans Active Directory peut être définie selon l'un des trois niveaux d'accès disponibles pour l'objet de groupe : KVM User (Utilisateur KVM), KVM User Admin (Administrateur d'utilisateur KVM) ou KVM Appliance Admin (Administrateur de matériel KVM). Les membres du groupe peuvent alors accéder aux matériels et aux équipements cibles au niveau d’accès spécifié.

Redémarrage du matériel

Après une telle mise à niveau, vous devrez peut-être redémarrer régulièrement l'équipement d'accès à distance SwitchView IP 1020.

Redémarrage à distance de l’équipement d’accès à distance SwitchView IP 1020 :

1. Dans la barre de navigation latérale, sélectionnez *Appliance* - *Overview* (Matériel - Vue d’ensemble).
2. Lorsque la fenêtre de la vue d’ensemble du matériel s’affiche, cliquez sur *Tools* - *Reboot Appliance* (Outils - Redémarrer le matériel).

Gestion des comptes locaux

L’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 offre des fonctions de sécurité locale et de connexion par l’intermédiaire de comptes utilisateurs définis par l’administrateur. La fonction *Local Accounts* de la barre de menus latérale permet aux administrateurs d’ajouter ou de supprimer des utilisateurs, de définir les niveaux de préemption et d’accès, et de modifier les mots de passe.

Niveaux d’accès

Lorsqu’un compte utilisateur est ajouté à l’interface Web intégrée, l’utilisateur peut se voir attribuer n’importe lequel des niveaux d’accès suivants :

- Administrateurs de matériel
- Administrateurs d’utilisateurs
- Utilisateurs

Tableau 3.4 : Opérations autorisées par niveau d’accès

	Niveau d’accès		
Opération	**Administrateur de matériel**	**Administrateur d’utilisateurs**	**Utilisateurs**
Configuration des paramètres du niveau système de l’interface Web intégrée	Oui	Non	Non
Configuration des droits d’accès	Oui	Oui	Non
Ajout, modification et suppression des comptes utilisateur	Oui, pour tous les niveaux d’accès	Oui, uniquement pour les utilisateurs et les administrateurs	Non
Modification du mot de passe de l’utilisateur	Oui	Oui	Oui
Accès à l’équipement cible	Oui, tous les équipements cibles	Oui, tous les équipements cibles	Oui, s’il est autorisé

Ajout d’un nouveau compte utilisateur (administrateur uniquement) :

1. Dans la barre de menus latérale, sélectionnez *Local Accounts*. La liste des utilisateurs s’affiche.
2. Cliquez sur le bouton *Add*.
3. Saisissez le nom et le mot de passe du nouvel utilisateur dans les espaces prévus à cet effet.

4. Sélectionnez les niveaux de préemption et d’accès.
5. Cliquez sur le bouton *Save* pour terminer le processus.

Suppression d’un compte utilisateur (administrateur uniquement) :

1. Dans la barre de menus latérale, sélectionnez *Local Accounts*. La liste des utilisateurs s’affiche.
2. Cochez la case située à gauche de chaque compte à supprimer puis cliquez sur le bouton *Delete*.

Modification d’un compte utilisateur (administrateur ou utilisateur actif uniquement) :

1. Dans la barre de menus latérale, sélectionnez *Local Accounts*. La liste des utilisateurs s’affiche.
2. Cliquez sur le nom de l’utilisateur dont le compte est à modifier. Un profil d’utilisateur s’affiche.
3. Modifier le compte utilisateur, puis cliquez sur *Save*.

Niveaux de préemption

Le niveau de préemption des utilisateurs détermine leur capacité ou non à déconnecter la session série ou vidéo (KVM) d’un autre utilisateur sur un équipement cible.

Les administrateurs de l’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 peuvent définir le niveau de préemption des utilisateurs à la création des comptes. Les niveaux de préemption vont de 1 à 4, le niveau le plus élevé étant 4. Par exemple, un utilisateur bénéficiant d’un niveau de préemption 4 peut préempter la session d’autres utilisateurs de niveau 4 ainsi que ceux ayant un niveau de 1, 2 ou 3.

CHAPITRE 4

Visualiseur vidéo

Fenêtre du visualiseur vidéo

Le visualiseur vidéo permet de mener une session KVM sur l'équipement cible relié à un équipement d'accès à distance SwitchView IP 1020. Lors de la connexion à un équipement à l'aide du visualiseur vidéo, le bureau de l'équipement cible s'affiche dans une nouvelle fenêtre, laquelle contient le curseur local et le curseur de l'équipement cible. Le visualiseur vidéo est compatible avec une souris à 3 ou 5 boutons.

Le logiciel de l'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 exécute un programme sur Java pour afficher la fenêtre du visualiseur vidéo. L'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 télécharge et installe automatiquement le visualiseur vidéo lors de sa première utilisation.

NOTA : En revanche, il n'installe pas l'utilitaire Java Resource Engine (JRE), lequel peut être téléchargé gratuitement à partir de http://www.sun.com pour les utilisateurs de PC et de http://www.apple.com pour les utilisateurs de Mac. En mode IPv4, l'application Java 1.5 (ou version ultérieure) est requise. En mode IPv6, l'application Java 1.6 (ou version ultérieure) est requise. Les systèmes d'exploitation MAC ne prennent pas en charge Java 1.5 pour l'instant et par conséquent, les utilisateurs de ces systèmes ne peuvent pas exécuter le mode IPv6.

NOTA : L'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 utilise la mémoire système pour stocker et afficher des images dans le visualiseur. Chaque fenêtre ouverte du visualiseur utilise de la mémoire système supplémentaire :

- Un paramètre couleur de 8 bits sur le PC client utilise 1,4 Mo de mémoire par fenêtre du visualiseur vidéo.
- Un paramètre de 16 bits utilise 2,4 Mo et un paramètre de 32 bits 6,8 Mo.

Si un autre utilisateur accède à l'équipement cible auquel vous souhaitez accéder, vous êtes invité à préempter la session de l'autre utilisateur à condition de bénéficier d'un niveau de préemption supérieur ou égal au sien. Les administrateurs de matériel peuvent également déconnecter un utilisateur actif sur la page Active Session (Session active).

Lancement d’une session KVM

NOTA : En cas d’utilisation d’une connexion sans proxy, les performances vidéo par une connexion réseau plus lente risquent de ne pas être optimales. Certains paramètres de couleur, tels que Grayscale (Nuances de gris), utilisent moins de bande passante réseau que d’autres, tels que Best Color (Jeu de couleurs optimal). Par conséquent, la modification des paramètres de couleur peut améliorer les performances vidéo. Pour des performances vidéo optimales sur une connexion réseau lente, Avocent recommande les paramètres Grayscale/Best Compression (Nuances de gris/Compression optimale) ou Low Color/High Compression (Couleurs faibles/Compression forte) Reportez-vous à la section *1024 x 768 768 x 576 960 x 720 704 x 528 896 x 672 640 x 480 832 x 624* à la page 34 pour de plus amples informations.

NOTA : Si un utilisateur se connecte à un équipement cible avec une résolution supérieure à celle de l'ordinateur local, la fenêtre du visualiseur vidéo contient uniquement une partie de l'écran de l'équipement cible et des barres de défilement pour afficher le reste de cet écran. L'utilisateur peut afficher l'écran dans son intégralité en réglant la résolution de l'équipement cible, de l'ordinateur local ou des deux.

Lancement d’une session KVM à partir de la fenêtre de l'explorateur du SwitchView IP 1020

1. Cliquez sur l’un des équipements de la liste dans l’écran Target Device (Équipement cible) pour ouvrir la fenêtre de vue d’ensemble de l’unité.
2. Cliquez sur *KVM Session* (Session KVM) pour ouvrir le visualiseur vidéo dans une nouvelle fenêtre.

Expiration de session

La session à distance peut expirer en cas d’inactivité de la fenêtre de session pendant une durée spécifiée. Le délai d’inactivité est configuré dans la fenêtre Appliance KVM Session Settings (Paramètres de la session KVM du matériel). La valeur attribuée au délai d’inactivité sera utilisée la prochaine fois qu’un utilisateur accèdera à l’interface Web intégrée du commutateur.

Activation et désactivation de l’expiration de la session :

1. Dans la barre de menus latérale, cliquez sur *Unit Views* - *Appliance* - *Appliance Settings* - *Sessions* - *KVM Settings* (Affichage des unités - Matériel - Paramètres du matériel - Sessions - Paramètres KVM).
2. Sélectionnez le paramètre de votre choix dans le champ *Enable Activity Timeout* (Activer délai d’inactivité).
3. Si nécessaire, sélectionnez une limite de temps d’inactivité.

Caractéristiques de la fenêtre du visualiseur vidéo

La Figure 4.1 présente les zones de la fenêtre du visualiseur vidéo. Les descriptions se trouvent dans le Tableau 4.1.

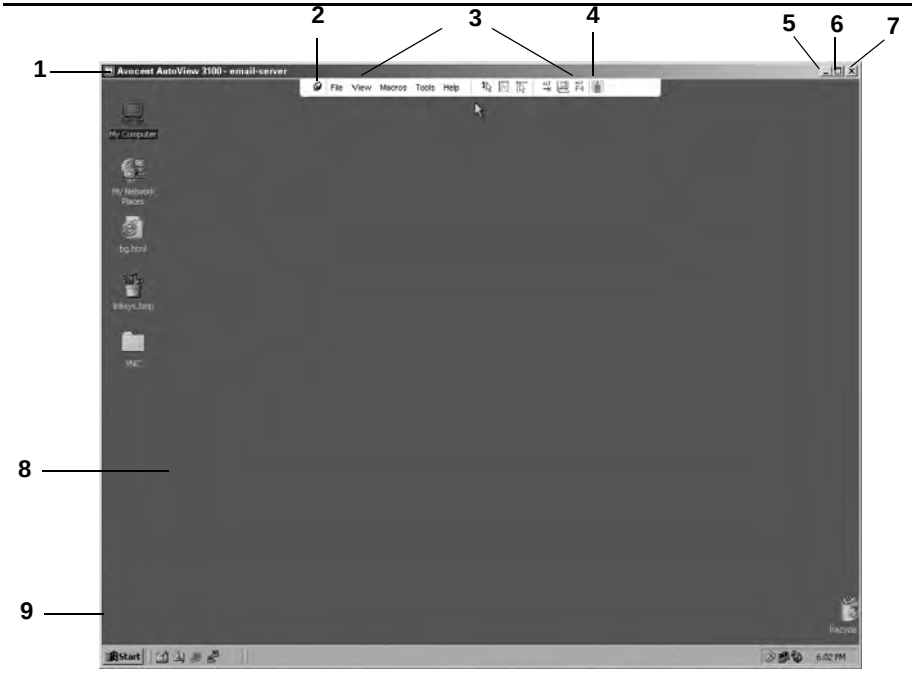

Figure 4.1 : Fenêtre du visualiseur vidéo (mode d'affichage normal)

Tableau 4.1 : Description de la Figure 5.1

Numéro	Description
1	Barre de titre : affiche le nom du serveur en cours de visualisation. En mode plein écran, la barre de titre disparaît et le nom du serveur s'affiche entre la barre de menus et la barre d'outils.
2	Punaise : verrouille l'affichage de la barre de menus et d'outils de manière à ce qu'elle soit toujours visible.
3	Barre de menus et d'outils : permet l'accès à de nombreuses fonctions du visualiseur vidéo. Si la punaise n'est pas activée, la barre de menus et d'outils est affichée/masquée. Placez le curseur sur la barre d'outils pour afficher la barre de menus et d'outils. La barre d'outils peut afficher jusqu'à dix boutons de commande et/ou de groupe de macros. Par défaut, les boutons Single Cursor Mode (Mode curseur unique), Refresh (Actualiser), Automatic Video Adjust (Réglage vidéo automatique) et Align Local Cursor (Aligner curseur local) apparaissent dans la barre d'outils. Pour plus d'informations, reportez-vous aux sections *Modification de la barre d'outils* à la page 32 et *Utilisation de macros* à la page 42.
4	Boutons de macros : combinaisons de touches régulièrement utilisées pouvant être envoyées à l'équipement cible.
5	Bouton Réduire : réduit l'affichage de la fenêtre du visualiseur vidéo à un bouton de la barre des tâches, en bas de l'écran de l'ordinateur local.

Tableau 4.1 : Description de la Figure 5.1 (suite)

Numéro	Description
6	Bouton Agrandir : fait passer la taille de la fenêtre au mode plein écran de manière à ce que le bureau de l'équipement visualisé s'affiche en plein écran. L'agrandissement de la fenêtre a les conséquences suivantes : • La barre de titre disparaît. • Le nom du serveur s'affiche entre la barre de menus et la barre d'outils. • Le bouton Agrandir se transforme en bouton Normal Window Mode (Mode d'affichage normal) qui apparaît dans la barre d'outils. Cliquez sur ce bouton pour basculer vers l'affichage normal de la fenêtre du visualiseur. • Le bouton Close (Fermer) s'affiche dans la barre d'outils.
7	Bouton Close : ferme la fenêtre du visualiseur vidéo. **NOTA :** Le bouton Close ne s'affiche pas sur tous les systèmes d'exploitation.
8	Bureau de l'équipement auquel vous accédez : communique avec l'équipement grâce à cette fenêtre.
9	Cadre : redimensionne la fenêtre du visualiseur lorsque vous cliquez et maintenez le bouton de la souris enfoncé sur le cadre.

Modification de la barre d'outils

Vous pouvez choisir le délai au bout duquel la barre d'outils est masquée lorsqu'elle se trouve dans l'état affichée/masquée (c'est-à-dire, non verrouillée à l'aide de la punaise).

Définition d'une durée de masquage de la barre d'outils :

1. Sélectionnez *Tools* - *Session Options* (Outils - Options de session) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Session Options*.

   La boîte de dialogue *Session Options* s'affiche.
2. Cliquez sur l'onglet *Toolbar* (Barre d'outils).
3. À l'aide des boutons fléchés, indiquez le délai en secondes avant le masquage de la barre d'outils.
4. Cliquez sur *OK* pour enregistrer les modifications et fermer la boîte de dialogue.

Réglage de la taille de la fenêtre

NOTA : La commande View - Scaling (Affichage - Mise à l'échelle) n'est pas disponible en mode plein écran ni aux utilisateurs secondaires d'une session partagée.

Lors de la première utilisation de l'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020, chaque fenêtre du visualiseur s'affiche par défaut avec une résolution de 1024 x 768. Cette résolution est conservée tant que vous ne la modifiez pas. Toutes les fenêtres du visualiseur peuvent avoir une résolution différente.

L’interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 règle automatiquement l’affichage si la taille de la fenêtre est modifiée au cours d’une session et à condition que la mise à l’échelle automatique soit activée. Si la résolution de l’équipement cible est modifiée en cours de session, l’affichage est automatiquement ajusté.

Modification de la résolution de la fenêtre du visualiseur vidéo :

1. Sélectionnez la commande *View - Scaling* (Affichage - Mise à l'échelle).
2. Cliquez sur la résolution de votre choix.

Réglage de l’affichage

Les menus et les boutons de la barre des tâches de la fenêtre du visualiseur permettent de réaliser les tâches suivantes :

- Aligner les curseurs de souris.
- Actualiser l’écran.
- Activer ou désactiver le mode plein écran. En mode plein écran, l’image est réglée pour que la résolution maximale du bureau soit de 1024 x 768. Si la résolution du bureau est supérieure :
  - L’image en plein écran est centrée sur le bureau et les zones entourant la fenêtre du visualiseur s’affichent en noir.
  - Les barres de menus et d’outils sont verrouillées de manière à être visibles à tout moment.
- Activer la mise à l’échelle automatique, totale ou manuelle de l’image de la session :
  - En mise à l’échelle totale, la fenêtre du bureau est fixe et l’image de l’équipement est redimensionnée à la taille de la fenêtre.
  - En mise à l’échelle automatique, la fenêtre du bureau est redimensionnée de manière à correspondre à la résolution du serveur visualisé.
  - En mise à l’échelle manuelle, un menu déroulant des résolutions prises en charge s’affiche.
- Modifier la profondeur d’échantillonnage de l’image d’une session

Alignement des curseurs de souris :

Cliquez sur le bouton *Align Local Cursor* (Aligner curseur local) de la barre d’outils du visualiseur vidéo. Le curseur local s’aligne alors avec le curseur de l’équipement distant.

NOTA : Si le curseur présente des problèmes d'alignement, désactivez le paramètre d'accélération de l'équipement relié.

Actualisation de l’écran :

Cliquez sur le bouton *Refresh Image* (Actualiser image) de la fenêtre du visualiseur.

-ou-

Sélectionnez *View - Refresh* (Affichage - Actualiser) dans la barre de menus du visualiseur vidéo.

L’image vidéo numérisée est alors entièrement régénérée.

Activation et désactivation du mode plein écran :

1. Pour activer le mode plein écran, cliquez sur le bouton *Agrandir.*
   -ou-
   Sélectionnez *View - Full Screen* (Affichage - Plein écran) dans la barre de menus du visualiseur vidéo.

   La fenêtre du bureau disparaît et seul le bureau de l'équipement auquel vous avez accès est visible. L'écran est agrandi jusqu'à un maximum de 1024 x 768. Si le bureau possède une résolution supérieure, un fond noir entoure l'image en plein écran. La barre d'outils flottante s'affiche.

   -ou-

2. Pour désactiver le mode plein écran et retourner à la fenêtre du bureau, cliquez sur le bouton *Full Screen Mode* (Mode plein écran) de la barre d'outils flottante.

Activation de la mise à l'échelle :

Pour activer la mise à l'échelle totale, sélectionnez *View - Scaling* (Affichage - Mise à l'échelle) dans la barre de menus du visualiseur vidéo. L'image de l'équipement est automatiquement redimensionnée à la résolution du serveur en cours de visualisation.

-ou-

Pour activer la mise à l'échelle manuelle, sélectionnez *View - Scaling* (Affichage - Mise à l'échelle) dans la barre de menus du visualiseur vidéo. Sélectionnez les dimensions pour redimensionner la fenêtre. Les résolutions suivantes sont disponibles pour la mise à l'échelle manuelle :

1024 x 768	768 x 576
960 x 720	704 x 528
896 x 672	640 x 480
832 x 624	

Réglage de la profondeur d'échantillonnage

L'algorithme Dambrackas Video Compression® (DVC) du commutateur AutoView permet de régler le nombre de couleurs visibles dans la fenêtre d'une session à distance. Vous pouvez choisir d'augmenter le nombre de couleurs pour une meilleure fidélité de reproduction ou de le diminuer afin de réduire le volume des données transmises sur le réseau.

Les paramètres d'affichage des fenêtres du visualiseur vidéo sont Best Color Available (actualisation plus lente), Best Compression (actualisation plus rapide), une combinaison des deux, ou Grayscale.

Pour définir la profondeur d'échantillonnage des voies et des canaux individuels, sélectionnez la commande *View - Color* (Affichage - Couleur) dans la fenêtre de la session à distance.

Réglage vidéo supplémentaire

En général, les fonctions de réglage automatique de la fenêtre du visualiseur donnent le meilleur affichage vidéo possible. Cependant, vous pouvez, sur recommandation d'un membre de l'équipe d'assistance technique d'Avocent, régler plus précisément la vidéo à l'aide de la commande *Tools - Manual Video Adjust* (Outils - Réglage vidéo manuel) de la barre de menus du visualiseur vidéo ou en cliquant sur le bouton *Manual Video Adjust* (Réglage vidéo manuel). La boîte de dialogue *Manual Video Adjust* s'affiche.

Vous pouvez vérifier le niveau de paquets par seconde nécessaire pour un écran statique en observant la vitesse affichée dans le coin inférieur droit de la boîte de dialogue.

Réglage manuel de la qualité vidéo de la fenêtre

NOTA : Les réglages vidéo suivants doivent être configurés uniquement sur recommandation et avec l'aide d'un membre de l'équipe d'assistance technique d'Avocent.

1. Sélectionnez *Tools - Manual Video Adjust* (Outils - Réglage vidéo manuel) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Manual Video Adjust*.

   La boîte de dialogue Manual Video Adjust représentée dans la Figure 4.2 s'affiche, les descriptions se trouvent dans le Tableau 4.2.

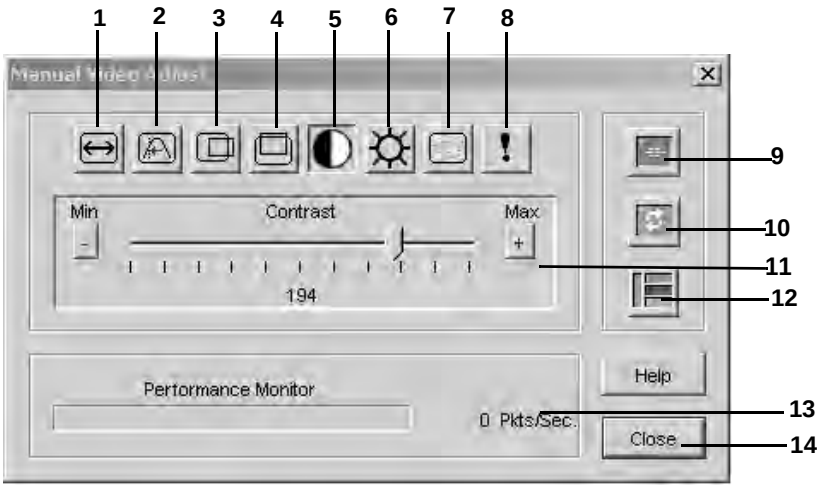

Figure 4.2 : Boîte de dialogue *Manual Video Adjust*

Tableau 4.2 : Descriptions de la Figure 5.2

Numéro	Description	Numéro	Description
1	Largeur de la capture d'image	**8**	Niveau sonore des pixels
2	Échantillon de pixels/réglage fin	**9**	Réglage vidéo automatique
3	Position horizontale de la capture d'image	**10**	Actualiser image
4	Position verticale de la capture d'image	**11**	Barre de réglage
5	Contraste	**12**	Modèle d'essai vidéo
6	Brillance	**13**	Indicateur de performance
7	Niveau sonore des blocs	**14**	Bouton Fermer

2. Cliquez sur l'icône correspondant à la fonction que vous souhaitez régler.
3. Déplacez le curseur de contraste, puis affinez le réglage en cliquant sur le bouton *Min* (-) ou *Max* (+) pour chaque paramètre sélectionné. Les réglages s'affichent immédiatement dans la fenêtre du visualiseur vidéo.
4. Lorsque vous avez terminé, cliquez sur *Close* pour quitter la boîte de dialogue *Manual Video Adjust*.

Paramètres vidéo cibles

Les commandes de réglage Capture Width (Largeur de la capture d'image), Pixel Sampling/Fine Adjust (Échantillon de pixels/réglage fin), Image Capture Horizontal Position (Position horizontale de la capture d'image) et Image Capture Vertical Position (Position verticale de la capture d'image) agissent sur la capture et la numérisation de l'image de l'équipement cible et sont rarement modifiées.

Les paramètres de capture d'image sont modifiés automatiquement par la fonction de réglage automatique. La cible doit avoir une image particulière afin d'effectuer des réglages indépendants précis.

Contraste et brillance

Si l'image de la fenêtre du visualiseur vidéo est trop sombre ou trop claire, sélectionnez *Tools - Automatic Video Adjust* (Outils - Réglage vidéo automatique) ou cliquez sur le bouton *Automatic Video Adjust* (Réglage vidéo automatique). Cette commande est également disponible dans la boîte de dialogue Video Adjustments (Réglages vidéo) Dans la plupart des cas, cette opération permet de corriger le problème.

Au cas où l'activation répétée de la commande de *réglage automatique* ne serait pas suffisante pour corriger le contraste et la luminosité, il peut être utile de les régler manuellement. Augmentez la brillance. Ne l'augmentez pas de plus de 10 incréments avant de passer au réglage du contraste. En général, le contraste nécessite peu de modifications.

Seuils de détection

Dans certains cas, le bruit de la transmission vidéo maintient le nombre de paquets par seconde à une valeur élevée, indiquée par l'apparition de petits points autour du curseur lorsqu'il se déplace. En modifiant les valeurs de seuil, l'affichage à l'écran et le repérage du curseur sont améliorés.

Si vous utilisez une compression vidéo standard, vous pouvez modifier les valeurs Noise Threshold (Niveau sonore) et Priority Threshold (Seuil de priorité). Vous pouvez également modifier les valeurs Block Noise Threshold (Niveau sonore des blocs) et Pixel Noise Threshold (Niveau sonore des pixels). Pour restaurer les valeurs de seuil par défaut, cliquez sur *Auto Adjust Video* (Réglage vidéo automatique).

Seuil de bruit des blocs et des pixels

Les valeurs Block Noise Threshold et Pixel Noise Threshold définissent les niveaux minimaux de couleur en termes de nombre autorisé de blocs vidéo et de pixels modifiés pour mille.

- Le paramètre Block Noise Threshold détermine la modification minimale de couleur dans un même bloc vidéo. L'augmentation de ce seuil réduit la bande passante du réseau. Sa diminution entraîne la réduction de la taille de ces artéfacts.
- Le paramètre Pixel Noise Threshold détermine la modification minimale de couleur dans un même pixel. L'augmentation de ce seuil réduit le nombre d'artéfacts de faible contraste mais augmente la bande passante du réseau.

Pour de plus amples informations sur la profondeur d'échantillonnage, reportez-vous à la section *Réglage de l'affichage* à la page 33.

Réglage vidéo automatique

Dans la plupart des cas, vous n'avez pas besoin de modifier les paramètres d'affichage vidéo par défaut. Le système ajuste et optimise automatiquement les paramètres d'affichage. L'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 offre les meilleures performances lorsque les paramètres d'affichage sont réglés de telle manière qu'aucun paquet de données vidéo (0) n'est transmis pour un écran statique.

Pour régler les paramètres vidéo sur des valeurs optimales, cliquez sur le bouton *Auto Adjust Video* de la boîte de dialogue Manual Video Adjust.

NOTA : Vous avez également la possibilité de régler automatiquement les paramètres vidéo en sélectionnant *Tools - Automatic Video Adjust* (Outils - Réglage vidéo automatique) dans la barre de menus du visualiseur ou en cliquant sur l'icône *Automatic Video Adjust* de la barre d'outils.

Actualiser image

Si vous cliquez sur le bouton *Refresh Image* de la boîte de dialogue Manual Video Adjust, l'image vidéo numérisée est entièrement régénérée.

NOTA : Pour actualiser l'image, sélectionnez *View - Refresh* (Affichage - Actualiser) dans la barre de menus du visualiseur vidéo.

Modèle d'essai vidéo

Pour basculer vers l'affichage d'un modèle d'essai vidéo, cliquez sur le bouton *Video Test Pattern* (Modèle d'essai vidéo) dans la boîte de dialogue Manual Video Adjust. Cliquez à nouveau sur ce bouton pour revenir à l'image vidéo *normale*.

Réglage des options de la souris

Les options de la souris du visualiseur concernent le type de curseur, le mode de curseur, la mise à l'échelle, l'alignement et la réinitialisation. Les paramètres de la souris s'appliquent à un équipement particulier, ils peuvent différer d'un équipement à un autre.

NOTA : Si l'équipement ne permet pas de débrancher et de rebrancher la souris (contrairement aux possibilités offertes par la plupart des PC récents), la souris est alors désactivée et l'équipement doit être redémarré.

Type de curseur

La fenêtre du visualiseur vidéo offre cinq options de curseur local. Vous avez également la possibilité de n'utiliser aucun curseur ou de garder le curseur par défaut.

En mode curseur simple, l'affichage du curseur local (secondaire) dans le visualiseur est désactivé et seul le pointeur de la souris de l'équipement cible est visible. Seuls les mouvements de la souris de l'équipement cible apparaissent à l'écran. Utilisez le mode curseur unique lorsqu'aucun curseur local n'est nécessaire. La Figure 4.3 illustre un curseur distant et un curseur local affichés dans la fenêtre du visualiseur vidéo.

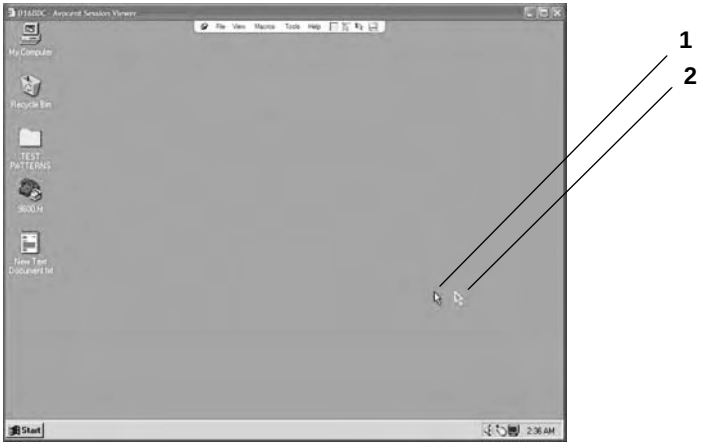

Figure 4.3 : Curseurs local et distant affichés dans la fenêtre du visualiseur vidéo

Tableau 4.3 : Descriptions de la Figure 5.3

Numéro	Description
1	Curseur distant
2	Curseur local

Le mode de curseur actif dans le visualiseur s'affiche dans la barre de titre, accompagné du raccourci clavier permettant de quitter le mode curseur unique. Vous pouvez définir ce raccourci clavier dans la boîte de dialogue Session Options.

NOTA : En cas d'utilisation d'un équipement capturant les frappes au clavier avant qu'elles n'atteignent le client, il est recommandé d'éviter d'utiliser ces frappes pour restaurer le pointeur de la souris.

Passage en mode Curseur unique :

Sélectionnez *Tools* - *Single Cursor Mode* (Outils - Mode curseur unique) dans la barre de menus du visualiseur vidéo.

-ou-

Cliquez sur le bouton *Single Cursor Mode* (Mode curseur unique).

Le curseur local ne s'affiche pas. Tous les mouvements observés sont ceux de l'équipement cible.

Sélection d'une touche pour quitter le mode curseur unique :

1. Sélectionnez *Tools* - *Session Options* (Outils - Options de session) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Session Options*.

   La boîte de dialogue Session Options s'affiche.
2. Cliquez sur l'onglet *Mouse* (Souris).
3. Sélectionnez un raccourci clavier de fin dans le menu déroulant de la zone Single Cursor (Curseur unique).
4. Cliquez sur *OK* pour enregistrer les paramètres.

Lorsque le mode curseur simple est activé, utilisez le raccourci clavier défini pour revenir au mode de bureau normal.

Quitter le mode curseur unique :

Appuyez sur la touche indiquée dans la barre de titre.

Modification du paramètre de curseur :

1. Sélectionnez *Tools - Session Options* (Outils - Options de session) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Session Options*.

   La boîte de dialogue Session Options s'affiche.
2. Cliquez sur l'onglet *Mouse*.
3. Sélectionnez un type de curseur dans le volet Local Cursor (Curseur local).
4. Cliquez sur *OK* pour enregistrer les paramètres.

Mise à l'échelle de la souris

Certaines versions antérieures de Linux ne prenaient pas en charge les accélérations de souris réglables. Pour les installations nécessitant une prise en charge de ces versions antérieures, vous pouvez choisir parmi trois options préconfigurées de mise à l'échelle de la souris ou définir vos propres paramètres. Les paramètres préconfigurés sont : Default (Défaut) (1:1), High (Élevé) (2:1) et Low (Faible) (1:2).

- Avec un rapport de mise à l'échelle de 1:1, tout mouvement de la souris dans la fenêtre du bureau envoie un mouvement de souris équivalent vers le serveur.
- Avec un rapport de 2:1, le même mouvement de souris envoie un mouvement de souris multiplié par 2.
- Avec un rapport de 1:2, le facteur de multiplication est de 1/2.

Réglage de mise à l'échelle de la souris :

1. Sélectionnez *Tools - Session Options* (Outils - Options de session) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Session Options*.

   La boîte de dialogue Session Options s'affiche.
2. Cliquez sur l'onglet *Mouse*.
3. Activez le bouton radio correspondant au paramètre préconfiguré de votre choix.
   -ou-
   Mise à l'échelle personnalisée :
   a. Cliquez sur le bouton radio *Custom* (Personnalisé) pour activer les champs X et Y.
   b. Saisissez une valeur de mise à l'échelle de la souris dans les champs X et Y. Pour toute entrée de la souris, les mouvements sont multipliés par les facteurs de mise à l'échelle X et Y respectivement. Les paramètres saisis doivent être compris entre 0,25 et 3,00.

Paramètres vidéo spécifiques aux fournisseurs

Les paramètres vidéo varient considérablement selon les fabricants. Avocent dispose d'une base de données en ligne contenant les paramètres vidéo optimisés de plusieurs cartes vidéo, en particulier ceux spécifiques à Sun. Pour obtenir ces informations, consultez la base de connaissances en ligne d'Avocent ou contactez le service d'assistance technique par téléphone.

Alignement et synchronisation de la souris

L'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020 ne pouvant recevoir de retour d'information de la souris en permanence, il peut arriver que la souris du système relié à l'équipement et la souris de l'hôte ne soient plus synchrones. Si la souris ou le clavier ne répondent plus correctement, il est parfois nécessaire d'aligner la souris ou de rétablir le repérage.

L'alignement permet d'aligner le curseur local avec le curseur du serveur distant. La réinitialisation entraîne une simulation de reconnexion de la souris et du clavier, comme si vous les aviez déconnectés puis reconnectés.

Réalignement de la souris :

Cliquez sur le bouton *Align Local Cursor* (Aligner curseur local) de la barre d'outils du visualiseur vidéo.

Transmission des frappes au clavier

Lorsque le visualiseur vidéo est lancé, les frappes au clavier peuvent être interprétées de deux manières selon le mode d'affichage de la fenêtre du visualiseur.

- En mode plein écran, toutes les frappes au clavier et les combinaisons de touches à l'exception de **Ctrl-Alt-Suppr** sont transmises au serveur distant en cours de visualisation.
- En mode d'affichage normal du bureau, la transmission des frappes au clavier permet de contrôler la reconnaissance par le serveur distant ou l'ordinateur local de certaines frappes ou combinaisons de touches.

La transmission des frappes au clavier est définie dans la boîte de dialogue Session Options. Lorsque cette option est activée et le visualiseur actif, toutes les frappes au clavier et les combinaisons de touches à l'exception de **Ctrl-Alt-Suppr** sont transmises au serveur distant en cours de visualisation. Lorsque le bureau local est actif, les frappes au clavier et les combinaisons de touches agissent sur l'ordinateur local.

NOTA : La combinaison **Ctrl-Alt-Suppr** peut être transmise au serveur distant uniquement à l'aide d'une macro.

NOTA : Sur les claviers japonais, la combinaison **ALT-Han/Zen** est toujours envoyée au serveur distant, quel que soit le mode d'affichage ou le paramètre de transmission des frappes au clavier.

Activation de la transmission des frappes au clavier :

1. Sélectionnez *Tools - Session Options* (Outils - Options de session) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Session Options*.

   La boîte de dialogue des options de session s'affiche.

2. Cliquez sur l'onglet *General* (Généralités).

3. Sélectionnez *Pass-through all keystrokes in regular window mode* (Transmission de toutes les combinaisons de touches en mode fenêtre normal).
4. Cliquez sur *OK* pour enregistrer les paramètres.

Utilisation de macros

Des macros pour les plates-formes Windows et Sun sont préconfigurées sur l'interface Web intégrée de l'équipement d'accès à distance SwitchView IP 1020.

Envoi d'une macro :

Sélectionnez *Macros* - <*macro de votre choix*> dans la barre de menus du visualiseur vidéo.

-ou-

Sélectionnez le bouton de la macro de votre choix dans la barre d'outils du visualiseur vidéo.

Enregistrement de l'image

Vous pouvez enregistrer l'image de la fenêtre du visualiseur dans un fichier ou dans le presse-papier puis le coller dans un programme de traitement de texte ou autre.

Capture d'une image de la fenêtre du visualiseur vidéo dans un fichier :

1. Sélectionnez *File* - *Capture to File* (Fichier - Copier dans un fichier) dans la barre de menus du visualiseur vidéo.
   -ou-
   Cliquez sur le bouton *Capture to File* (Copier dans un fichier).

   La boîte de dialogue Save As (Enregistrer sous) s'affiche.
2. Saisissez un nom de fichier et un emplacement d'enregistrement.
3. Cliquez sur *Save* (Enregistrer) pour enregistrer l'image dans un fichier.

Capture d'une image de la fenêtre du visualiseur vidéo dans le presse-papier :

Sélectionnez *File* - *Capture to Clipboard* (Fichier - Copier dans presse-papier) dans la barre de menus du visualiseur vidéo.

-ou-

Cliquez sur le bouton *Capture to Clipboard* (Copier dans presse-papier).

L'image est enregistrée dans le presse-papier.

Fermeture d'une session du visualiseur vidéo

Fermeture d'une session du visualiseur vidéo :

Sélectionnez *File* - *Exit* (Fichier - Quitter) dans la barre de menus du visualiseur vidéo.

ANNEXES

Annexe A : Mises à jour Flash

L'option de mise à jour Flash de l'équipement d'accès à distance SwitchView IP 1020 vous permet d'actualiser votre matériel avec le dernier firmware disponible.

Une fois la mémoire Flash mise à niveau, l'équipement d'accès à distance SwitchView IP 1020 redémarre à chaud, interrompant ainsi toutes les sessions de module IQ. Un équipement cible dont le firmware de module IQ est en cours de mise à jour risque de ne pas s'afficher ou d'être signalé comme déconnecté. L'équipement cible est normalement à nouveau visible dès la mise à jour Flash terminée.

ATTENTION : La déconnexion ou la mise sous tension puis hors tension du SwitchView IP 1020 lors de la mise à jour pourrait le rendre inopérationnel ; vous devrez alors utiliser la procédure de récupération pour le reprogrammer.

Mise à jour du firmware de l'équipement d'accès à distance SwitchView IP 1020 :

1. Pour télécharger la version la plus récente du firmware Flash d'Avocent, visitez la page http://www.avocent.com/support. Enregistrez le fichier de mise à jour Flash dans le répertoire approprié d'un ordinateur pouvant accéder à l'équipement d'accès à distance SwitchView IP 1020.
2. Si l'équipement d'accès à distance SwitchView IP 1020 est hors tension, mettez-le sous tension. Patientez une minute environ avant de vous connecter.
3. Sélectionnez *Firmware Management (Gestion du firmware)* pour afficher la version actuelle du firmware dans le menu Firmware Management.
4. Cliquez sur le bouton *Upgrade Firmware (Mise à jour du firmware)*.
5. Sélectionnez le répertoire et le fichier appropriés à l'aide du navigateur.
6. Cliquez sur le bouton *Upgrade (Mettre à jour)*.
7. L'équipement d'accès à distance SwitchView IP 1020 lance la procédure de mise à jour Flash. Des indicateurs s'affichent à l'écran pour vous permettre de suivre l'évolution de l'opération. Lorsque la mise à jour est terminée, le SwitchView IP 1020 se réinitialise et met à jour les sous-systèmes internes.
8. Une fois la mise à jour terminée, l'écran de connexion apparaît.

NOTA : Si le voyant vert du panneau arrière de l'équipement clignote, cela signifie que l'équipement est en mode de récupération.

Récupération d’une mise à jour Flash :

NOTA : Si vous ne disposez pas d’un serveur TFTP, différents sharewares et freewares peuvent être téléchargés.

1. Pour télécharger la version la plus récente du firmware Flash d’Avocent, visitez la page http://www.avocent.com/support. Enregistrez le fichier de mise à jour Flash dans le répertoire approprié du serveur TFTP.
2. Indiquez l’adresse IP 192.168.1 pour le serveur TFTP.
3. Renommer le fichier de téléchargement svip1020.fl et placez-le dans le répertoire de base TFTP du serveur TFTP.
4. Assurez-vous que l’équipement SwitchView IP 1020 est sous tension.

Le processus de récupération devrait démarrer automatiquement.

Annexe B : Spécifications techniques

Tableau B.1 : Spécifications produit de l'équipement d'accès à distance SwitchView IP 1020

Voies du serveur	
Nombre	1
Type	PS/2, USB
Connecteurs	PS/2, USB, VGA
Types de synchronisation	Horizontale et verticale séparées
Plug and Play	DDC2B
Résolution vidéo	640 x 480 à 60 Hz 800 x 600 à 75 Hz 960 x 700 à 75 Hz 1024 x 768 à 75 Hz Résolution maximum : 1280 x 1024 à 75 Hz (voie distante)
Câblage compatible	Câble CPS2-6A de 1,8 m
Dimensions	
Hauteur x Largeur x Profondeur	2,70 cm x 20,80 cm x 13,34 cm
Poids (sans les câbles)	0,68 kg sans les câbles
Connexion réseau	
Nombre	1
Type	Ethernet 10/100/1000
Connecteur	RJ-45
Voie locale	
Nombre	1
Type	PS/2, VGA
Consommation d'énergie	5 W
Tension d'alimentation	Alimentation externe 5 VCC à 2,0 A
Puissance d'alimentation (c.a.)	10,5 W maximum (120 V, 60 Hz)

Tableau B.1 : Spécifications produit de l'équipement d'accès à distance SwitchView IP 1020 (suite)

Tension d'alimentation en courant alternatif	100 - 240 V.c.a.
Fréquence d'alimentation	Auto-détection 50 à 60 Hz
Courant nominal d'alimentation (c.a.)	0,5 A
Câble d'alimentation (c.a.)	1,8 m, 2 conducteurs, 18 AWG
Conditions atmosphériques ambiantes	
Humidité	Fonctionnement et stockage : 5 à 95 % sans condensation
Températures	Fonctionnement : de 0 à 40 °C Hors fonctionnement : -30 à 70 °C
Certifications et labels de sécurité et normes EMC	UL, FCC, cUL, ICES-003, CE, VCCI, MIC, C-Tick Les certifications de sécurité et EMC de ce produit portent différents noms : CMN (Certification Model Number ou Numéro de modèle de conformité), MPN (Manufacturer's Part Number ou Numéro de référence du fabricant) ou Sales Level Model (Modèle de niveau de vente). Le nom faisant référence aux rapports et certificats EMC et/ou de sécurité est imprimé sur l'étiquette du produit.

Annexe C : Émulation des touches avancées du clavier Sun

Il est possible d'émuler certaines touches d'un clavier Sun (US) de type 5 standard en utilisant des combinaisons de touches sur un clavier PS/2. Pour activer le mode d'émulation de touches avancées du clavier Sun et utiliser ces raccourcis clavier, maintenez les touches **Ctrl+Maj+Alt** enfoncées, puis appuyez sur la touche **Arrêt défil**. Le voyant *Arrêt défil* se met à clignoter. Utilisez la touche indiquée dans le Tableau C.1 comme si vous utilisiez les touches avancées sur un clavier Sun.

Tableau C.1 : Émulation des touches du clavier Sun

Touche Sun (US)	Touche PS/2 activant l'émulation des touches Sun
Composer	Application(1)
Composer	Pavé numérique
Alimentation	F11
Ouvrir	F7
Aide	Verr Num
Props	F3
Devant	F5
Stop	F1
Encore	F2
Annuler	F4
Couper	F10
Copier	F6
Coller	F8
Cher.	F9
Silence	Touche / du pavé numérique
Vol +	Touche + du pavé numérique
Vol -	Touche - du pave numérique
Commande (gauche)(2)	F12
Commande (gauche)(2)	Touche Windows gauche (1)
Commande (droite)(2)	Touche Windows droite (1)

(1) Clavier Windows 95 à 104 touches.
(2) La touche Commande est la touche Sun Meta (représentant un losange).

Par exemple : Pour **Stop + A**, maintenez les touches **Ctrl+Maj+Alt** enfoncées et appuyez sur Arrêt défil, puis sur **F1 + A**.

Ces combinaisons de touches fonctionnent avec le module IQ USB (si votre système Sun est équipé d’une voie USB), ainsi qu’avec les modules VSN et WSN IQ Sun. À l’exception de la touche **F12**, ces raccourcis clavier ne sont pas reconnus sous Microsoft Windows. La touche **F12** exécute l’activation d’une touche Windows.

Une fois l'opération terminée, maintenez les touches **Ctrl+Maj+Alt** enfoncées, puis appuyez sur la touche **Arrêt défil** pour désactiver l’émulation des touches avancées du clavier Sun.

Remarques spéciales concernant les claviers USB Sun japonais et coréens (modules IQ USB uniquement)

Les claviers USB Sun japonais et coréens attribuent des ID d’utilisation à certaines touches qui diffèrent des ID d’utilisation USB standard. Si des modules IQ USB sont reliés à vos serveurs Sun, vous devez utiliser des touches alternatives pour les touches Han/Zen et Katakana/Hiragana des claviers USB Sun japonais et les touches Hangul et Hanja des claviers USB Sun coréens.

Ces différences de claviers peuvent entraîner des incohérences de mappage du clavier lors de la commutation entre les équipements cibles utilisant des modules IQ VSN et WSN Sun et des équipements cibles utilisant les modules IQ USB. Ces touches fonctionnent normalement si vos serveurs Sun sont reliés à l'équipement d'accès à distance SwitchView IP 1020 via un module IQ VSN ou WSN.

Le Tableau C.2 décrit le mappage du clavier lors de l’utilisation d’un module IQ USB.

Tableau C.2 : Mappages de touches PS/2-USB

Clavier PS/2	ID d’utilisateur USB	Clavier Sun USB	Clavier Sun USB coréen	Clavier Sun USB japonais
Alt Gr	0xE6	Alt. Graph.	Hangul	Katakana/Hiragana
Application Windows	0x65	Composer	Hanja	Composer
Hangul	0x90	Sans objet	N/A	N/A
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35	` ~	` ~	N/A

Annexe D : Réinitialisation de l'équipement aux valeurs par défaut

Réinitialisation de l'équipement d'accès à distance SwitchView IP 1020 aux valeurs par défaut :

1. Repérez le petit orifice situé sur la partie droite de l'équipement SwitchView IP 1020.
2. Introduisez-y une épingle puis appuyez sur le bouton de réinitialisation et maintenez le enfoncé pendant 3 secondes.

NOTA : L'équipement d'accès à distance SwitchView IP 1020 redémarre alors et toutes les connexions sont perdues.

3. Le voyant bleu du panneau avant de l'équipement SwitchView IP 1020 clignote, indiquant que l'équipement est en cours de reprogrammation.
4. Une fois les valeurs par défaut réinitialisées, connectez-vous à nouveau à cet équipement.

NOTA : Par défaut, le nom d'utilisateur est Admin et il n'y a pas de mot de passe.

Annexe E : Assistance technique

Notre équipe d’assistance technique se tient à votre disposition en cas de problème d’installation ou de fonctionnement susceptible de se produire avec un produit Avocent. Si vous rencontrez une difficulté, procédez comme suit pour bénéficier d’une aide le plus rapidement possible.

Remédier à un problème :

1. Vérifiez la section appropriée du manuel pour voir si le problème peut être résolu à l’aide des procédures indiquées.
2. Consultez le site http://www.avocent.com/support et effectuez une recherche dans la base de connaissances ou utilisez le formulaire d’aide en ligne.
3. Appelez le service d’assistance technique Avocent le plus proche.

Avocent

The Power of Being There

For Technical Support:

www.avocent.com/support

590-538-616E